ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA SCIENTIARUM MATHEMATICARUM

ADIUVANTIBUS

L. KALMÁR ET L. RÉDEI

REDIGIT

B. SZ.-NAGY

TOMUS XIX

FASC. 1—2

SZEGED, 1958

INSTITUTUM BOLYAIANUM UNIVERSITATIS SZEGEDIENSIS

A SZEGEDI TUDOMÁNYEGYETEM KÖZLEMÉNYEI

ACTA SCIENTIARUM MATHEMATICARUM

KALMÁR LÁSZLÓ ÉS RÉDEI LÁSZLÓ
KÖZREMŰKÖDÉSÉVEL
SZERKESZTI
SZŐKEFALVI-NAGY BÉLA

19. KÖTET
1—2. FÜZET

INDEX — TARTALOM

SZEGED, 1958. JÚNIUS HÓ

SZEGEDI TUDOMÁNYEGYETEM BOLYAI-INTÉZETE

ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA SCIENTIARUM MATHEMATICARUM

ADIUVANTIBUS
L. KALMÁR ET L. RÉDEI
REDIGIT
B. SZ.-NAGY

TOMUS XIX
1958

SZEGED

INSTITUTUM BOLYAIANUM UNIVERSITATIS SZEGEDIENSIS

A SZEGEDI TUDOMÁNYEGYETEM KÖZLEMÉNYEI

ACTA SCIENTIARUM MATHEMATICARUM

KALMÁR LÁSZLÓ és RÉDEI LÁSZLÓ
KÖZREMŰKÖDÉSÉVEL
SZERKESZTI
SZŐKEFALVI-NAGY BÉLA

19. KÖTET
1958

SZEGED

SZEGEDI TUDOMÁNYEGYETEM BOLYAI-INTÉZETE

INDEX — TARTALOM

TOMUS XIX — 1958 — 19. KÖTET

BIBLIOGRAPHIE

A kiadásért felelős:
Szökefalvi-Nagy Béla
Eredeti kiadásról készült változatlan utánnyomás

Külföldi terjesztés:
KULTURA KÖNYV- ÉS HÍRLAP
KÜLKERESKEDELMI VÁLLALAT
BUDAPEST 62,
P. O. B. 149
This book is a reproduction of the original, published in Budapest

General Distributors:
KULTURA Hungarian Trading Company
for Books and Newspapers
BUDAPEST 62, P. O. B. 149,
Hungary
Printed in Hungary, 1968

68-2043 - Felsőoktatási Jegyzetellátó Vállalat

An elementary semigroup theorem and a congruence relation of Rédei.

By ŠTEFAN SCHWARZ in Bratislava (ČSR).

RÉDEI proved the following theorem: Let $m > 1$ be an integer, $\varphi(m)$ the Euler function. Then every integer x satisfies the relation

$$x^m \equiv x^{m-\varphi(m)} \pmod{m}. \tag{1}$$

If $m = p$ is a prime, (1) has the form $x^p \equiv x \pmod{p}$; hence (1) is a generalization of the theorem of FERMAT.

An elementary proof of (1) is given in [1], p. 132.

The purpose of this note is to show that (1) is a special case of a general theorem concerning finite semigroups.

The proof of (1) based on the theory of semigroups seems to be of some interest, since in spite of advances of the theory of semigroups in the last years non-trivial applications to the elementary theory of numbers are rather sporadic.

For convenience of the reader we recall in section 1 some elementary facts concerning finite semigroups. The general theorem mentioned above will be given in section 2. In section 3 we give the application to the proof of RÉDEI's theorem.

1.

Let S be a finite semigroup and $a \in S$. The sequence

$$a, a^2, a^3, \ldots \tag{2}$$

contains a finite number of different elements. Denote by $\varrho(a)$ and $\sigma(a)$, the smallest integers with $a^{\varrho(a)} = a^{\sigma(a)}$, $\varrho(a) < \sigma(a)$. It is well known that (2) contains then exactly $\sigma(a) - 1$ different elements. These are

$$a, a^2, \ldots, a^{\varrho(a)-1}, a^{\varrho(a)}, \ldots, a^{\sigma(a)-1}. \tag{3}$$

The set $\{a^{\varrho(a)}, \ldots, a^{\sigma(a)-1}\} = \mathfrak{g}_a$ is a group. The number $l_a = \sigma(a) - \varrho(a)$ will

be called the period of a. For every $\lambda \geqq \varrho(a)$ the element a^λ is contained in $\mathfrak{g}_a$ and $a^\lambda = a^{\lambda+\tau l_a}$ holds for all integers $\tau > 0$.

The set (3) contains exactly one idempotent e, namely, the unit of $\mathfrak{g}_a$. We shall say that a belongs to the idempotent e.

Denote by P_e the set of all elements $\in S$ belonging to a fixed idempotent e. Then S can be written as the class sum of disjoint subsets $S = \sum P_e$, where e runs through all idempotents $\in S$.

To every e there exists a unique maximal group G_e having e as unit element. Cleary $G_e \subseteqq P_e$. The group G_e contains exactly all $x \in P_e$ for which $xe = ex = x$ holds. It is therefore $e \cdot P_e = P_e \cdot e = G_e$.

If S contains a unit element e_1 (more generally a one-sided unit element e_1), then $P_{e_1} \cdot e_1 = P_{e_1}$, hence $P_{e_1} = G_{e_1}$, i. e. the set of elements $\in S$ belonging to the unit element (one-sided unit element) forms a group.

2.

Let now be S a finite semigroup of order $m > 1$ with a two-sided unit e_1 and the corresponding maximal group G_1.

We shall show: If S is not a group, then $S - G_1$ is a semigroup. This assertion is known. Nevertheless we give a short proof. Let be $b \in S - G_1$. We prove first $Sb \cap G_1 = \mathfrak{0}$. The proof follows indirectly. Suppose $a \in Sb \cap G_1$. Then there is a b^* with $a = b^* b$. Find an $a^* \in G_1$ with $a^* a = e_1$. Then $a^* b^* b = e_1$. Denote $c = a^* b^*$; then $cb = e_1$. Since $b \in S - G_1$, b belongs to an idempotent $e' \neq e_1$, i. e. there exists an integer $\varrho > 0$ such that $b^\varrho = e' \neq e_1$. The relation $cb = e_1$ implies $c(cb) \cdot b = ce_1 b = cb = e_1, c^2 b^2 = e_1$. Repeating this argument we have $c^\varrho b^\varrho = e_1$, i. e. $c^\varrho e' = e_1$. Hence $e_1 = c^\varrho e' = c^\varrho (e' e') = (c^\varrho e') e' = e_1 e' = e'$, which is a contradiction. For every $b \in S - G_1$ we have $Sb \subset S - G_1$, hence $S(S - G_1) \subset S - G_1$ and the more $(S - G_1)^2 \subset S - G_1$. This shows that $S - G_1$ is a semigroup.

Denote the order of G_1 by l.

Suppose first $x \in G_1$. Then $x^l = e_1$. If $m > l$ we have $x^{m-l} \in G_1$. Hence $x^{m-l} \cdot e_1 = x^{m-l}$. On the other side we have $x^{m-l} \cdot e_1 = x^{m-l} \cdot x^l = x^m$. Therefore

$$x^m = x^{m-l}.$$

(This result holds also for $m = l$, if x^0 denotes the unit element of G_1.)

Suppose for the rest that $m > l$ and $x \in S - G_1$. The semigroup $S - G_1$ is of order $m - l$. Hence the set

(4) $$x, x^2, \ldots, x^{m-l}$$

contains (a unique) idempotent e. There exists therefore an integer k,

$1 \leqq k \leqq m-l$, with $x^k = e$. The intersection of the maximal group G_e with the set (4) is the group $\mathfrak{g}_x$. Since $k \leqq m-l$, we have $x^{m-l} \in \mathfrak{g}_x$. If l_x is the period of x there holds

$$x^{m-l} = x^{m-l+\tau l_x}$$

for every non-negative integer τ.

Suppose now that l_x is a divisor of l. Then there is a $\tau \geqq 1$ such that $-l+\tau l_x = 0$. Hence $x^{m-l} = x^m$.

Thus we have proved:

Theorem. *Let S be a finite semigroup of order m having a unit element e_1. Denote by l the order of the maximal group belonging to e_1. If the period of every $x \in S$ is a divisor of l, then*

$$x^m = x^{m-l}$$

holds for every $x \in S$.

Remark. This theorem can be generalized as follows. Suppose that S has exactly s right units. It is known (see [2] and [3]) that the maximal groups $G_1^{(1)}, \ldots, G_1^{(s)}$ belonging to these idempotents are isomorphic and the set $S-(G_1^{(1)}+\cdots+G_1^{(s)})$ is a semigroup. (In fact it is an ideal of S.) An analogous argument as above shows the validity of the following theorem:

Let S has exactly s right units and let l be the (common) order of the maximal groups belonging to each of them. If the period of all $x \in S$ divides ls, then every $x \in S$ satisfies the relation $x^m = x^{m-sl}$.

3.

We shall show now that the theorem of RÉDEI is a special case of our theorem.

Let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_1 > 0, \ldots, \alpha_r > 0$ be the factorization of $m > 0$ into different primes. Let S_m be the semigroup of residue classes (mod m). The class containing the number x will be denoted by $[x]$.

The maximal group belonging to $[1]$ is the set of all $[a] \in S_m$ with $(a, m) = 1$. Its order is $\varphi(m)$. To prove (1) it is sufficient to show that *the period of each $[x] \in S_m$ divides $\varphi(m)$.*

Let be $[x] \in S_m$. By rearranging suitably the primes we can suppose that $[x]$ is of the form

$$[x] = [p_1^{k_1} \cdots p_s^{k_s} a],\ 0 \leqq s \leqq r,\ k_1 \geqq 1, \ldots, k_s \geqq 1,$$

with $(a, m) = 1$. (The case $s = 0$ means $[x] = [a]$ with $(a, m) = 1$. In this case

$[x]$ is an element of a group of order $\varphi(m)$ and our assertion is trivially true.) The relation $[x]^\varrho = [x]^\sigma$ with $1 \leqq \varrho \leqq \sigma$ implies

$$(p_1^{k_1} \cdots p_s^{k_s} a)^\varrho = (p_1^{k_1} \cdots p_s^{k_s} a)^\sigma \pmod m,$$

i. e.

$$(5) \qquad (p_1^{k_1} \cdots p_s^{k_s} a)^\varrho \{(p_1^{k_1} \cdots p_s^{k_s} a)^{\sigma-\varrho} - 1\} \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}.$$

a) If $s = r$, then there exists such a $\varrho > 0$ that

$$(p_1^{k_1} \cdots p_r^{k_r} a)^\varrho \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}.$$

Let ϱ_1 be the smallest such ϱ. The relation $[x]^{\varrho_1} = [0]$ implies $[x]^{\varrho_1+1} = [x]^{\varrho_1}$. All elements of the form considered have the period equal to 1 and our assertion is true.

b) Suppose $0 < s < r$. To satisfy (5) we must first choose ϱ such that

$$(p_1^{k_1} \cdots p_s^{k_s})^\varrho \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_s^{\alpha_s}}.$$

Let ϱ_1 be the smallest such ϱ. The congruence (5) will then be satisfied if and only if $\sigma > \varrho_1$ is such that

$$(6) \qquad (p_1^{k_1} \cdots p_s^{k_s} a)^{\sigma-\varrho_1} - 1 \equiv 0 \pmod{p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r}}.$$

But $(p_1^{k_1} \cdots p_s^{k_s} a, p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r}) = 1$. Denote by σ_1 the smallest σ satisfying (6). Then $\sigma_1 - \varrho_1$ is either $\varphi(p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r})$ or a divisor of this number. Hence $\sigma_1 - \varrho_1$ divides $\varphi(m)$, i. e. the period of every element $[x] \in S_m$ divides $\varphi(m)$, q. e. d.

References.

[1] W. Sierpiński, *Arytmetyka teoreticzna* (Warszawa, 1955).

[2] Št. Schwarz, Topological semigroups with one-sided units, *Czechoslovak Math. Journal*, **5 (80)** (1955), 153-163.

[3] W. M. Faucett—R. J. Koch—K. Numakura, Complements of maximal ideals in compact semigroups, *Duke Math. Journal*, **22** (1955), 655-662.

(Received September 23, 1957.)

Über die Punktmengen der Divergenz der singulären Integrale von Riemann-integrablen Funktionen.

Von H. ZAHORSKA in Łódź (Polen).

In dieser Arbeit werden wir notwendige und hinreichende Bedingungen für die Menge N aller Punkte x des Intervalls (a, b) angeben, in denen das singuläre Integral

$$\lim_{r\to\infty} \int_a^b K(r, t-x) f(t)\, dt = \lim_{r\to\infty} \int_a^b K(r, t) f(x+t)\, dt$$

nicht existiert, wo der Kern $K(r, t)$ die Bedingungen von FADDEEFF erfüllt und die Funktion $f(x)$ Riemann-integrabel ist. (Unter gewissen Bedingungen existieren diese Grenzwerte für $a < x < b$ gleichzeitig und sie sind gleich.)

Die Notwendigkeit der Bedingungen wird bei schwächeren Voraussetzungen bewiesen. Und zwar, der Kern $K(r, x, t)$ braucht nicht die Gestalt $K(r, t-x)$ besitzen und die Faddeeffschen Bedingungen erfüllen, es genügt, daß er quasipositiv ist.

Der Beweis des Hinreichens der Bedingungen besteht in der Konstruktion einer entsprechenden Funktion $f(x)$. Dabei kann man eine und dieselbe Funktion $f(x)$ für eine beliebige endliche Anzahl von singulären Integralen konstruieren, so daß diese alle in den Punkten der gegebenen Menge N divergent und in allen Punkten der Komplementärmenge CN zu $f(x)$ konvergent sind. Dabei darf man den Grenzübergang $r \to \infty$ für jedes einzelne singuläre Integral im allgemeinen in einer anderen Wertmenge von r vornehmen.

Notwendige Bedingungen.

Es sei $K(r, x, t)$ eine für jedes feste $r > 0$ und $x \in [a, b]$ in $[a, b]$ Lebesgue-integrierbare Funktion von t. Man sagt, $K(r, x, t)$ sei ein *quasipositiver* Kern, wenn die folgenden Bedingungen erfüllt sind:

a) $\lim_{r\to\infty} \int_a^b K(r, x, t)\, dt = 1$; b) $\int_a^b |K(r, x, t)|\, dt < H(x)$,

wo $H(x)$ eine endliche positive, von r unabhängige Funktion in $[a, b]$ ist;

$$\text{c)} \quad \lim_{r\to\infty}\left(\int_a^{x-\delta} + \int_{x+\delta}^{b}\right)|K(r,x,t)|\,dt = 0$$

für jedes $\delta > 0$.

Es ist bekannt, daß jeder quasipositive Kern die Eigenschaft besitzt, daß wenn man

$$Q(r,x) = \int_a^b K(r,x,t)f(t)\,dt$$

setzt, in jedem Stetigkeitspunkt $x_0 \in [a, b]$ der Funktion $f(x)$ gilt: $\lim_{r\to\infty} Q(r, x_0) = f(x_0)$. Unter gewissen Voraussetzungen über $K(r, x, t)$ ist $Q(r, x)$ eine stetige Funktion von x in $[a, b]$[1]), folglich ist die Menge N aller Punkte x, für die $\lim_{r\to\infty} Q(r, x)$ nicht existiert, von der Klasse $G_{\delta\sigma}$ (vgl. HAUSDORFF [2]). Aus der Quasipositivität folgt, daß N in der Menge K aller Unstetigkeitspunkte der Funktion $f(x)$ enthalten ist; die Menge K ist von der Klasse F_σ und ist für Riemann-integrable Funktionen $f(x)$ vom Maß 0. Daraus folgt leicht:

$$(1) \qquad N = \sum_{k=1}^{\infty} N_k, \quad N_k \in G_\delta, \quad |\bar{N}_k| = 0 \quad \text{und} \quad N_k \cdot N_l = 0 \quad \text{für} \quad k \neq l.^{2})$$

(Der Beweis dieser Behauptung ist in meiner Arbeit [3] angegeben.)

Hinreichende Bedingungen.

In folgendem werden wir den folgenden Hilfssatz benötigen.

Hilfssatz. (Verallgemeinerter Satz von LUSIN—MENCHOFF.) *Für jede meßbare Menge A und abgeschlossene Mengen B, F mit $B \subset \cdot A$ und $F \subset \cdot A$,*[3]) *und für jede nicht abnehmende positive Funktion $\delta(l)$ existiert eine abge-*

---

[1]) Das bedeutet eine Voraussetzung über $K(r, x, t)$, wenn wir im allgemeinen Fall keine stärkere Voraussetzungen machen wollen, wie z. B. gleichmäßige (in Bezug auf t) Stetigkeit in $[a, b]$ nach x, oder Stetigkeit in $[a, b]$ nach x und eine Ungleichung $|K(r, x, t)| \leqq \varphi(r)$ für jedes $r > 0$, $x \in [a, b]$, $t \in [a, b]$, wo $\varphi(r)$ eine für $r > 0$ endliche Funktion ist, etc. Im Falle $K(r, x, t) = K(r, t-x)$ sind diese Voraussetzungen unnötig; für beschränkte meßbare Funktionen $f(x)$ und nach t Lebesgue-integrable $K(r, t)$ ist $Q(r, x)$ stetig nach x.

[2]) Im allgemeinen bezeichnet $\bar{N}$ die abgeschlossene Hülle von N, $|N|$ bezeichnet das Lebesguesche Maß von N, und $N \in G_\delta$ bezeichnet, daß die Menge N von der Klasse G_δ ist.

[3]) $C \subset \cdot D$ bedeutet, daß $C \subset D$ und C lauter aus Dichtigkeitspunkten von D besteht.

schlossene Menge E mit den Eigenschaften:

$$B \subset \cdot E \subset \cdot A, \quad F \subset E, \quad B \operatorname{int} A \subset \operatorname{int} E,$$

$$\frac{|(x, x+h)\cdot E|}{|h|} > \frac{|(x, x+h)\cdot A|}{|h|} - \delta\left(\frac{1}{m}\right) \text{ für jedes } x \in B \text{ und } |h| < \frac{1}{m}$$ [4])

(m eine beliebige natürliche Zahl).

(Der Beweis des Hilfssatzes befindet sich in meiner Arbeit [3].)

Es sei $a < 0 < b$. Wir betrachten ein endliches System $K_i(r, t)$ $(i = 1, 2, 3, \ldots, n)$ von für jedes positive r in $[a, b]$ Lebesgue-integrierbaren Funktionen, das die folgenden Bedingungen erfüllt:

I. $\int_a^b K_i(r, t)\, dt = 1; \qquad K_i(r, t) = 0$ für $t \overline{\in} [a, b] \quad (i = 1, 2, \ldots, n);$

II. $\lim_{r \to \infty} \left(\int_a^{-\delta} + \int_{\delta}^{b} \right) |K_i(r, t)|\, dt = 0$ für jedes feste $\delta > 0$ und $i;$

III. es existiert eine solche Funktion $F(r, t)$ (die sogenannte Majorante von FADDEEFF), daß $|K_i(r, t)| < F(r, t)$ für $i = 1, 2, \ldots, n$ gilt, $F(r, t)$ als Funktion von t in $[a, 0]$ nicht abnehmend und in $[0, b]$ nicht zunehmend ist, ferner

$$\int_a^b F(r, t)\, dt$$

unter einer von r unabhängigen positiven Konstante C bleibt.

Wir setzen für eine in $[a, b]$ beschränkte, Lebesgue-integrierbare Funktion $f(x)$ mit der Periode $b - a$

$$Q_i(r, x) = \int_a^b K_i(r, t) f(x+t)\, dt \qquad (i = 1, 2, \ldots, n).$$

Wir werden den folgenden Satz beweisen.

Satz. *Für jedes Kernsystem $K_i(r, t)$ $(i = 1, 2, \ldots, n)$, das die Bedingungen* I, II, III *erfüllt, für jede Menge N $(\subset [a, b])$ von reellen Zahlen, die die Bedingungen* (1) *erfüllt, und für beliebig vorgegebene nach oben nicht beschränkte Mengen R_i von reellen Zahlen $(i = 1, 2, \ldots, n)$ existiert eine in $[a, b]$ beschränkte, Riemann-integrierbare Funktion $f(x)$, mit der Periode $b - a$, so daß*

$$\limsup_{r \in R_i,\, r \to \infty} Q_i(r, x) - \liminf_{r \in R_i,\, r \to \infty} Q_i(r, x) > 0$$

für $x \in N$ und

$$\lim_{r \to \infty} Q_i(r, x) = f(x)$$

für $x \in CN$ gilt $(i = 1, 2, \ldots, n)$.

---

[4]) Hier soll (α, β) dasselbe wie (β, α) bedeuten (offenes Intervall) wenn wir nicht wissen, ob $\alpha < \beta$ oder $\alpha > \beta$ ist; int A bezeichnet den offenen Kern der Menge A.

Beweis. Zuerst werden wir den Beweis für den Sonderfall $N \in G_\delta$ und $|\bar{N}| = 0$ durchführen. Da die Mengen R_i nach oben nicht beschränkt sind, kann man eine wachsende unendliche Folge $\{r_k\}$ so bestimmen, daß die Bedingungen

$$r_{mn+i} \in R_i \qquad (m = 0, 1, 2, \ldots;\ i = 1, 2, \ldots, n),$$

$$r_{mn+i} > 2^{m+1} \qquad (m = 0.\ 1, 2, \ldots)$$

erfüllt sind.

Wir bestimmen die Funktion $\alpha(s)$ folgendermaßen: es sei $m(s)$ die kleinste natürliche Zahl, für die im Falle $m \geqq m(s)$

$$\left(\int_a^{-s} + \int_s^b\right) |K_i(r_{mn+i}, t)|\,dt < 0{,}2 \qquad (i = 1, 2, \ldots, n) \tag{2}$$

gilt. Eine solche Zahl existiert für jedes $s > 0$, da die Kerne $K_i(r, t)$ die Bedingung II erfüllen. Wir bezeichnen für jedes $r > 0$ und $i = 1, 2, \ldots, n$ mit $\eta_i(r)$ die größte positive Zahl, die die folgende Bedingung erfüllt: für eine beliebige Menge M ($\subset [a, b]$) vom Maß $< \eta_i(r)$ gilt

$$\int_M |K_i(r, t)|\,dt < 0{,}1,$$

und wir setzen für jedes $s > 0$

$$\eta^*(s) = \min_{1 \leqq i \leqq n} \eta_i(r_{m(s)n+i}).$$

So erhalten wir für jede Menge M mit $|M| < \eta^*(s)$ $(s > 0)$

$$\int_M |K_i(r_{m(s)n+i}, t)|\,dt < 0{,}1 \qquad (i = 1, 2, \ldots, n). \tag{3}$$

Aus (2) und (3) ergibt sich $\eta^*(s) < 2s$; im entgegensetzten Fall wäre ja

$$\int_a^b |K_i(r_{m(s)n+i}, t)|\,dt < 0{,}3,$$

was der Bedingung I widerspricht.

Wir setzen

$$\alpha(s) = \begin{cases} \inf\limits_{s \leqq x \leqq 1} \dfrac{\eta^*(x)}{2x} & \text{für} \quad s \leqq 1, \\ \dfrac{\eta^*(1)}{2} & \text{für} \quad s > 1. \end{cases} \tag{4}$$

Die Funktion $\alpha(s)$ ist offenbar nicht abnehmend. Sie ist auch positiv. Im entgegengesetzten Fall gäbe es nämlich ein s_0 $(0 < s_0 < 1)$ mit $\alpha(s_0) = 0$, also nach (4) mit

$$\inf_{s_0 \leqq x \leqq 1} \eta^*(x) = 0. \tag{5}$$

Für $x \geqq s_0$ ist aber $m(s_0) \geqq m(x)$ und so gilt

$$\inf_{s_0 \leqq x \leqq 1} \eta^*(x) \geqq \min_{\substack{1 \leqq m \leqq m(s_0) \\ 1 \leqq i \leqq n}} \eta_i(r_{mn+i}) > 0,$$

im Gegensatz zu (5). Aus (4) folgt außerdem für jedes positive s,

$$\alpha(s) \leqq \frac{\eta^*(s)}{2s} < 1. \tag{6}$$

Mit Hilfe der Funktion $\alpha(s)$ soll die Funktion $\delta(l)$ bestimmt werden, mit der wir den verallgemeinerten Satz von LUSIN—MENCHOFF anwenden. Es sei $\delta(l) = \alpha(2^{-2}l)$ für $l > 0$. Dann ist $\delta(l)$ für $l > 0$ positiv und nicht abnehmend.

Nach der Voraussetzung ist $N \in G_\delta$ und $|\bar{N}| = 0$. Also ist

$$N = \prod_{k=1}^{\infty} G_k,$$

wo die G_k ($\subset [a, b]$) offene Mengen sind. Setzen wir $F_k = CG_k$, wo CG_k die Menge $[a, b] - G_k$ bezeichnet, so ist

$$CN = \sum_{k=1}^{\infty} F_k. \tag{7}$$

Wir bestimmen mit vollständiger Induktion eine Folge $\{L_k\}$ von abgeschlossenen Mengen von $[a, b]$ derart, daß die folgenden Bedingungen erfüllt sind:

$$\sum_{k=1}^{\infty} L_k = CN, \tag{8}$$

$$\begin{cases} L_{p-1} \subset \cdot L_p \subset \cdot CN \quad \text{für} \quad p = 2, 3, \ldots, \quad F_p \subset L_p \quad \text{für} \quad p = 1, 2, \ldots, \\ L_{p-1} \cdot C\bar{N} \subset \operatorname{int} L_p \quad \text{für} \quad p = 2, 3, \ldots, \\ \dfrac{|(x, x+h) \cdot L_p|}{|h|} > 1 - \delta\left(\dfrac{1}{m}\right) \quad \text{für} \quad x \in L_{p-1} \quad \text{und} \quad |h| < \dfrac{1}{m}, \; p = 2, 3, \ldots, \end{cases} \tag{9}$$

wo m eine beliebige natürliche Zahl ist und $\delta(l)$ die oben definierte Funktion bezeichnet.

Wir setzen $L_1 = F_1 = CG_1$. Es sei (mit den Bezeichnungen des Hilfssatzes) $CN = A$, $L_1 = B$ und $F_2 = F$. Es existiert also nach dem Hilfssatz eine abgeschlossene Menge $E = L_2$ mit den Eigenschaften

$$L_1 \subset \cdot L_2 \subset \cdot CN, \quad F_2 \subset L_2, \quad L_1 \cdot C\bar{N} = L_1 \cdot \operatorname{int} CN \subset \operatorname{int} L_2$$

und

$$\frac{|(x, x+h) \cdot L_2|}{|h|} > 1 - \delta\left(\frac{1}{m}\right) \quad \text{für jedes } x \in L_1 \text{ und } |h| < \frac{1}{m},$$

wo m eine beliebige natürliche Zahl ist.

Es sei k ($\geqq 2$) eine beliebige natürliche Zahl. Wir nehmen an, daß die Mengen $L_1, L_2, \ldots, L_k$ schon definiert sind, derart, daß die Bedingungen (9) für $p=1,2,\ldots,k$ erfüllt werden. Wir wenden den Hilfssatz mit der oben bestimmten Funktion $\delta(l)$ an, mit den Bezeichnungen $CN=A$, $L_k=B$ und $F_{k+1}=F$. Nach dem Hilfssatz gibt es eine Menge $E=L_{k+1}$ mit den Eigenschaften: $L_k \subset \cdot L_{k+1} \subset \cdot CN$, $F_{k+1} \subset L_{k+1}$, $C\bar{N} \cdot L_k \subset \operatorname{int} L_{k+1}$, und $|h|^{-1} \cdot |(x, x+h) \cdot L_{k+1}| > 1 - \delta\left(\frac{1}{m}\right)$ für $x \in L_k$ und $|h| < \frac{1}{m}$. Infolgedessen sind die Bedingungen (9) für $p=k+1$ erfüllt. Mit vollständiger Induktion erhalten wir auf diese Weise eine Mengenfolge $\{L_k\}$, für die die Bedingung (9) erfüllt wird. Da nach (7), (9)

$$CN = \sum_{k=1}^{\infty} F_k \subset \sum_{k=1}^{\infty} L_k \subset CN$$

besteht, so gilt auch (8).

Wir bestimmen jetzt die abgeschlossenen Mengen $L_{\frac{m}{2^k}}$ für jede natürliche m und ganze nicht negative k, welche die Ungleichung $m \geqq 2^k$ erfüllen, derart, daß die folgenden Bedingungen erfüllt sind:

$$L_{\frac{m_1}{2^k}} \subset \cdot L_{\frac{m_2}{2^k}} \quad \text{für} \quad m_1 < m_2, \tag{10}$$

$$L_{\frac{m_1}{2^k}} \cdot \operatorname{int} L_{\frac{m_3}{2^k}} \subset \operatorname{int} L_{\frac{m_2}{2^k}} \quad \text{für} \quad m_1 < m_2 < m_3. \tag{11}$$

Es sei $L_{\frac{m}{2^0}} = L_m$ $(m=1,2,\ldots)$. Offensichtlich sind diese Bedingungen für $k=0$ nach (9) erfüllt. Es sei k ($\geqq 0$) eine beliebige ganze Zahl. Nehmen wir an, daß die abgeschlossenen Mengen $L_{\frac{m}{2^k}}$ $(m \geqq 2^k)$ schon definiert wurden, derart, daß die Bedingungen (10) und (11) erfüllt sind. Wir bestimmen die Mengen $L_{\frac{m}{2^{k+1}}}$ wie folgt. Es sei $L_{\frac{2r}{2^{k+1}}} = L_{\frac{r}{2^k}}$ $(r=2^k, 2^k+1, \ldots)$. Mit Anwendung des Hilfssatzes ergibt sich eine abgeschlossene Menge $E=L_{\frac{2r+1}{2^{k+1}}}$, für die die Relationen

$$L_{\frac{r}{2^k}} \subset \cdot L_{\frac{2r+1}{2^{k+1}}} \subset \cdot L_{\frac{r+1}{2^k}} \quad \text{und} \quad L_{\frac{r}{2^k}} \cdot \operatorname{int} L_{\frac{r+1}{2^k}} \subset \operatorname{int} L_{\frac{2r+1}{2^{k+1}}}$$

bestehen, d. h. (10) und (11) für $k+1$ anstatt k. Also können diese Mengen für jede natürliche Zahl k mit vollständiger Induktion bestimmt werden. Sie erfüllen also nach (10), (11) auch die Bedingungen

$$L_{\frac{m}{2^k}} \subset \cdot L_{\frac{v}{2^r}} \quad \text{für} \quad \frac{m}{2^k} < \frac{v}{2^r}, \tag{12}$$

$$L_{\frac{p}{2^l}} \cdot \operatorname{int} L_{\frac{r}{2^r}} \subset \operatorname{int} L_{\frac{m}{2^k}} \quad \text{für} \quad 1 \leqq \frac{p}{2^l} < \frac{m}{2^k} < \frac{r}{2^r}. \tag{13}$$

Wir setzen endlich für jedes reelle $\lambda \geqq 1$

$$L_\lambda = \prod_{\frac{m}{2^k} \geqq \lambda} L_{\frac{m}{2^k}}. \tag{14}$$

Die Mengen L_λ sind abgeschlossen und erfüllen die Bedingungen

$$L_{\lambda_0} \subset \cdot L_{\lambda_1} \quad \text{für} \quad 1 \leqq \lambda_0 < \lambda_1, \tag{15}$$

$$L_{\lambda_0} \cdot \operatorname{int} L_{\lambda_2} \subset \operatorname{int} L_{\lambda_1} \quad \text{für} \quad 1 \leqq \lambda_0 < \lambda_1 < \lambda_2, \tag{16}$$

dabei stimmt für $\lambda = 2^{-k} m$ die Definition von L_λ mit der vorhergehenden überein.

Tatsächlich, die Formel (14) zieht $L_{\lambda_1} \subset L_{\lambda_2}$ für $\lambda_1 < \lambda_2$ nach sich. Wir wählen drei rationale Zahlen, deren Nenner Potenzen von 2 sind, derart, daß die Ungleichungen $\lambda_0 < \frac{p}{2^l} < \frac{m}{2^k} < \lambda_1 < \lambda_2 < \frac{r}{2^r}$ bestehen. Dann erhalten wir nach (13) $L_{\lambda_0} \cdot \operatorname{int} L_{\lambda_2} \subset L_{\frac{p}{2^l}} \cdot \operatorname{int} L_{\frac{r}{2^r}} \subset \operatorname{int} L_{\frac{m}{2^k}} \subset \operatorname{int} L_{\lambda_1}$, also ist (16) bewiesen, und nach (12) gilt $L_{\lambda_0} \subset L_{\frac{p}{2^l}} \subset \cdot L_{\frac{m}{2^k}} \subset L_{\lambda_1}$, woraus (15) folgt.

Es sei für jedes $x \in CN$

$$\omega(x) = \inf_{\lambda} E\{x \in L_\lambda\}. \tag{17}$$

Wir beweisen, daß $\omega(x)$ in CN endlich und approximativ stetig, in $C\bar{N}$ stetig ist. Offensichtlich ist nach (8) $\omega(x)$ endlich in CN. Es gilt $\omega(x) \leqq k$ für $x \in L_k$ und $\omega(x) \geqq k$ für $x \bar{\in} L_k$, demnach ist

$$k \leqq \omega(x) \leqq k+1 \quad \text{für} \quad x \in L_{k+1} - L_k. \tag{18}$$

Für ein beliebiges $x_0 \in CN$ betrachten wir die Zahl $\omega(x_0) - \varepsilon$, wo ε eine beliebige positive Zahl ist. Nach (17) erhalten wir $x_0 \bar{\in} L_{\omega(x_0)-\varepsilon}$, also ist $\operatorname{dist}(x_0, L_{\omega(x_0)-\varepsilon}) = \delta(x_0, \varepsilon) > 0$,[5]) und nach (15) ist $\operatorname{dist}(x_0, L_\lambda) \geqq \delta(x_0, \varepsilon) > 0$ für jedes $\lambda \leqq \omega(x_0) - \varepsilon$. Es liegen also von den Punkten $x \in CN$ im Intervall $(x_0 - \delta, x_0 + \delta)$ $(\delta = \delta(x_0, \varepsilon))$ nur jene, welche zu L_λ mit $\lambda > \omega(x_0) - \varepsilon$ gehören, und so ist nach (17) $\omega(x) \geqq \omega(x_0) - \varepsilon$ für jedes $x \in (x_0 - \delta, x_0 + \delta) \cdot CN$, d. h. $\omega(x)$ ist halbstetig von unten auf CN im Punkt x_0. Betrachten wir jetzt die Zahl $\omega(x_0) + \frac{\varepsilon}{2}$. Nach (17) und (15) erhalten wir $x_0 \in L_{\omega(x_0)+\frac{\varepsilon}{2}} \subset \cdot L_{\omega(x_0)+\varepsilon}$. Für $x \in L_{\omega(x_0)+\varepsilon}$ ist $\omega(x) \leqq \omega(x_0) + \varepsilon$ nach (17), also ist der Punkt x_0 ein Dichtigkeitspunkt der Menge $E_x[\omega(x) \leqq \omega(x_0) + \varepsilon]$, d. h. $\omega(x)$ ist approximativ halbstetig von oben im Punkt x_0. Da $|N| = 0$ ist, so ist $\omega(x)$ nach den obigen approximativ stetig in CN.

[5]) Im allgemeinen bezeichnet dist (a, A) die Entfernung des Punktes a von der Menge A.

Ist $x_0 \in C\bar{N} = \operatorname{int} CN \subset CN$, so gilt $x_0 \in L_{\omega(x_0)+\frac{\varepsilon}{2}}$ und $x_0 \in L_k$, wo k eine natürliche Zahl $> \omega(x_0)+\varepsilon$ ist. Nach (9) ist dann $x_0 \in \operatorname{int} L_{k+1}$. Auf Grund von $x_0 \in L_{\omega(x_0)+\frac{\varepsilon}{2}}$ und $k+1 > \omega(x_0)+\varepsilon > \omega(x_0)+\frac{\varepsilon}{2}$ gilt also nach (16) $x_0 \in \operatorname{int} L_{\omega(x_0)+\varepsilon}$. Es existiert daher ein solches $\eta > 0$, daß $(x_0-\eta, x_0+\eta) \subset \subset L_{\omega(x_0)+\varepsilon}$ ist. Dann ist $\omega(x) \leqq \omega(x_0)+\varepsilon$ für jedes $x \in (x_0-\eta, x_0+\eta)$, d. h. $\omega(x)$ ist halbstetig von oben in x_0. Daraus folgt nach den obigen, auf Grund der Abgeschlossenheit von $\bar{N}$, daß $\omega(x)$ in allen Punkten von $C\bar{N}$ stetig ist.

Die Funktion $\omega(x)$ ist fast überall bestimmt, und zwar für jeden Punkt von CN. Durch beliebige Bestimmung der Werte von $\omega(x)$ in den übrigen Punkten wird ihre approximative Stetigkeit in den Punkten der Menge CN nicht verändert. Auch ihre Stetigkeit in den Punkten der Menge $C\bar{N}$ ändert sich nicht, da eine gewisse Umgebung dieser Punkte zu $C\bar{N}$, daher auch zu CN gehört, d. h. die Funktion $\omega(x)$ ist in diesen Umgebungen bestimmt und die zusätzliche Bestimmung in N (in den übrigen Punkten) die Werte in diesen Umgebungen nicht betrifft. (Man kann so nur die Halbstetigkeit der Funktion $\omega(x)$ von unten in $CN-C\bar{N}$ ändern. Man kann beweisen, daß wenn wir z. B. $\omega(x) = \text{const.}$ in N setzen, wird $\omega(x)$ in allen Punkten von N halbstetig von unten, das ist aber für diese Arbeit nicht nötig.)

Setzen wir endlich $\omega(x) = 1$ für $x \in N$; dann ist $\omega(x)$ überall in $[a, b]$ bestimmt und endlich.

Wir bestimmen für $y \geqq 1$ eine stetige Funktion $d(y)$. Es sei $d(1) = 1$, $d(y) = 2k+1$ für jedes $y \in [2k, 2k+1]$, $k = 1, 2, \ldots$, und linear in den übrigen Intervallen. Sie ist nicht abnehmend. Es sei

$$\Omega(x) = d[\omega(x)].$$

Die Funktion $\Omega(x)$ ist überall bestimmt, endlich, approximativ stetig in CN und stetig in $C\bar{N}$. Nachdem $\omega(x) \geqq 1$ ist, erfüllt $\Omega(x)$ nach (18) die Bedingung

$$\Omega(x) = 2k+1 \quad \text{für jedes} \quad x \in L_{2k+1}-L_{2k}. \tag{19}$$

Jetzt kann mann die Funktion $f(x) = a(x)$ bestimmen: es sei

$$a(x) = \sin \frac{\pi}{2} \Omega(x). \tag{20}$$

Nehmen wir an, daß $a(x)$ mit der Periode $b-a$ periodisch fortgesetzt ist. Diese Funktion ist überall bestimmt, beschränkt, stetig in $C\bar{N}$ und approximativ stetig in CN, also ist Riemann-integrabel, dabei ist nach (19) und (20)

$$a(x) = 1 \quad \text{für} \quad x \in L_{4k+1}-L_{4k}, \tag{21}$$

$$a(x) = -1 \quad \text{für} \quad x \in L_{4k+3}-L_{4k+2}. \tag{22}$$

Die Punkte der approximativen Stetigkeit einer beschränkten Funktion sind bekanntlich ihre Lebesgueschen Punkte. Daraus folgt nach dem Satz von FADDEEFF [1], daß

$$\lim_{r\to\infty}\int_a^b K_i(r,t)a(x+t)dt = a(x) \quad \text{für} \quad x\in CN, \quad i=1,2,\ldots,n \tag{23}$$

gilt, da nach I, II, III die Kerne $K_i(r,t)$ $(i=1,2,\ldots,n)$ die Voraussetzungen des Satzes von FADDEEFF erfüllen.

Wir beweisen, daß für jedes $x\in N$ die Grenze (23) nicht existiert. Es sei $x\in N$. Wir erhalten dann $x\in \prod_{k=1}^{\infty} CL_k$, $CL_{4k+1}\subset CL_{4k}$ $(k=1,2,\ldots)$, und $\lim_{k\to\infty}|CL_{4k}|=0$, also gelten $\operatorname{dist}(x,L_k)=d_k(x)>0$, $d_{k+1}(x)\leqq d_k(x)$ $(k=1,2,\ldots)$ und $\lim_{k\to\infty} d_k(x)=0$, da für $k\to\infty$, $|CL_k|\to 0$ ist. Wir betrachten die Folgen $\{L_{4k-1}\}$, $\{L_{4k+1}\}$.

Wir bezeichnen $d_{4k}(x)=u_k'=u$, und $m[d_{4k}(x)]=m_k'=m'$. Nach (2) erhalten wir

$$\left|\left(\int_a^{-u}+\int_u^b\right)K_i(r_{m'n+i},t)a(x+t)\,dt\right| \leqq \left(\int_a^{-u}+\int_u^b\right)|K_i(r_{m'n+i},t)|\,dt<0{,}2 \tag{24}$$

$$\text{für} \quad i=1,2,\ldots,n.$$

Wenigstens eine der Zahlen $x-u$, $x+u$ gehört zu L_{4k} und es gilt

$$(x-u,x+u)\subset CL_{4k}, \tag{25}$$

(da $u=\operatorname{dist}(x,L_{4k})$ ist). Es sei z. B. $x+u\in L_{4k}$. Wir schätzen das Maß $r=r_k$ der Menge $(x-u,x+u)\cdot CL_{4k+1}$ ab. Wegen $u=u_k'=d_{4k}(x)\to 0$ gibt es für jedes genügend große k eine natürliche Zahl m mit $\frac{1}{m+2}\leqq 2u<\frac{1}{m+1}$. Da $x+u\in L_{4k}$ ist, so gilt nach (9)

$$\frac{|(x-u,x+u)\cdot L_{4k+1}|}{2u}>1-\delta\left(\frac{1}{m+1}\right). \tag{26}$$

Daraus folgt $\frac{1}{m+1}<\frac{2}{m+2}\leqq 4u$. Wir erhalten also für genügend großes k

$$\delta\left(\frac{1}{m+1}\right)\leqq\delta(4u)=\alpha(2^{-2}\cdot 4u)=\alpha(u), \qquad 1-\delta\left(\frac{1}{m+1}\right)\geqq 1-\alpha(u),$$

woraus nach (26) folgt

$$\frac{|(x-u,x+u)\cdot L_{4k+1}|}{2u}>1-\alpha(u). \tag{27}$$

Da $(x-u,x+u)\cdot L_{4k+1}+(x-u,x+u)\cdot CL_{4k+1}=(x-u,x+u)$ ist, so erhalten

wir nach (27) $2^{-1}u^{-1}\cdot|(x-u, x+u)\cdot CL_{4k+1}| < \alpha(u)$, d. h. ist $\nu < 2u\alpha(u)$ für genügend große k. Diese Formel und (6) ergeben für genügend große k:

$$\nu < \eta^*(u).$$

Aus (3) erhalten wir für genügend große k:

$$\left|\int_{M_1} K_i(r_{m'n+i}, t)a(x+t)dt\right| \leqq \int_{M_1} |K_i(r_{m'n+i}, t)|dt < 0{,}1 \tag{28}$$

$(i=1, 2, \ldots, n)$, wo M_1 aus jenen Punkten t besteht, für welche $x+t \in (x-u, x+u)\cdot CL_{4k+1}$ gilt. Nach (25) ist

$$(x-u, x+u)\cdot(L_{4k+1}-L_{4k}) = (x-u, x+u)\cdot L_{4k+1}. \tag{29}$$

Nach (28) und (24) gilt für genügend große k:

$$\int_a^b K_i(r_{m'n+i}, t)a(x+t)\,dt \geqq \left(-\int_a^{-u} - \int_u^b\right)|K_i(r_{m'n+i}, t)|dt - \tag{30}$$

$$-\int_{M_1}|K_i(r_{m'n+i}, t)|\,dt + \int_{M_2} K_i(r_{m'n+i}, t)\,dt > \int_{M_2} K_i(r_{m'n+i}, t)\,dt - 0{,}3$$

$(i=1, 2, \ldots, n)$, wo M_2 die Menge derjenigen Punkte t bedeutet, für welche $x+t \in (x-u, x+u)\cdot L_{4k+1}$ ist, da nach (21) und (29) $a(x+t)=1$ für jedes $t \in M_2$ gilt. Auf analoge Weise folgt aus I, (28) und (24) für genügend große k und für $i=1, 2, \ldots, n$

$$\int_{M_2} K_i(r_{m'n+i}, t)\,dt \geqq \int_a^b K_i(r_{m'n+i}, t)\,dt - \left(\int_a^{-u} + \int_u^b\right)|K_i(r_{m'n+i}, t)|\,dt -$$

$$-\int_{M_1}|K_i(r_{m'n+i}, t)|\,dt > 1-0{,}3 = 0{,}7,$$

also nach (30) haben wir für $i=1, 2, \ldots, n$:

$$\int_a^b K_i(r_{m'n+i}, t)\cdot a(x+t)\,dt > 0{,}7-0{,}3 = 0{,}4.$$

Auf Grund von (22) beweisen wir die analoge Ungleichung für $m''=m[d_{4k+2}(x)]$ und für genügend große k:

$$\int_a^b K_i(r_{m''n+i}, t)a(x+t)\,dt < -0{,}4 \qquad (i=1, 2, \ldots, n).$$

Die Indexe $m'=m'_k$, $m''=m''_k$ sind nicht abnehmende und nicht beschränkte Funktionen von k, denn im entgegengesetzten Fall wäre nach (24) für einen gewissen Wert m_0 und u von beliebiger Kleinheit (da $u=d_{4k}(x)\to 0$, oder $u=d_{4k+2}(x)\to 0$ bei $k\to\infty$)

$$\left(\int_a^{-u} + \int_u^b\right)|K_i(r_{m_0n+i}, t)|\,dt < 0{,}2,$$

was mit I im Widerspruch steht.

Auf diese Weise haben wir zwei solche Folgen $r_{m'_k n+i} \to \infty$, $r_{m''_k n+i} \to \infty$, $(m'_k \to \infty, m''_k \to \infty$ bei $k \to \infty)$ bestimmt, daß $\limsup_{k\to\infty} Q_i(r_{m'_k n+i}, x) \geqq 0{,}4$ und $\liminf_{k\to\infty} Q_i(r_{m''_k n+i}, x) \leqq -0{,}4$ $(r_{m'_k n+i} \in R_i,\ r_{m''_k n+i} \in R_i)$ für jedes $x \in N$ und $i = 1, 2, \ldots, n$ besteht. Daraus folgt $\limsup_{r\to\infty} Q_i(r, x) - \liminf_{r\to\infty} Q_i(r, x) \geqq 0{,}8$ $(r \in R_i)$ für $x \in N$ und $i = 1, 2, \ldots, n$.

Der Satz ist also für den Spezialfall $N \in G_\delta$ bewiesen. Im allgemeinen Fall haben wir $N = \sum_{k=1}^{\infty} N_k$, wo $N_k \in G_\delta$, $N_k \cdot N_l = 0$ für $k \neq l$ und $|\bar{N}_k| = 0$ $(k = 1, 2, \ldots)$ ist. Es existiert also nach dem betrachteten Spezialfall für jedes natürliche k eine in $[a, b]$ Riemann-integrable Funktion $a_k(x)$ mit $|a_k(x)| \leqq 1$, die periodisch mit der Periode $b-a$ ist, und für welche die Operationen (die singulären Integrale) konvergent zu $a_k(x)$ auf CN_k und divergent auf N_k sind.

Wir werden zeigen, daß die Funktion

$$f(x) = \sum_{k=1}^{\infty} 2^{-k} a_k(x) \tag{31}$$

alle Bedingungen des Satzes erfüllt.

Es sei $x \in CN$, d. h. $x \in CN_k$ für jedes k. Dann hat man für $i = 1, 2, \ldots, n$:

$$\lim_{r\to\infty} \int_a^b K_i(r, t) a_k(x+t)\, dt = a_k(x). \tag{32}$$

Wir beweisen, daß für $i = 1, 2, \ldots, n$ auch

$$\lim_{r\to\infty} \int_a^b K_i(r, t) f(x+t)\, dt = f(x) \tag{33}$$

gilt. Nach I und III ist für jedes positive r

$$1 = \int_a^b K_i(r, t)\, dt \leqq \int_a^b |K_i(r, t)|\, dt \leqq C.$$

Also, gilt $|\varphi(x)| \leqq C_1$ für jedes $x \in [a, b]$, so hat man für jedes positive r

$$\left| \int_a^b K_i(r, t) \varphi(x+t)\, dt \right| \leqq C_1 C.$$

Es sei ε eine beliebige positive Zahl. Wir wählen $k_0(\varepsilon) = k_0$ derart, daß $2^{-k_0} \leqq \varepsilon \cdot 2^{-2} C^{-1}$ gilt. Dan ist für jedes $r > 0$

$$\left| \int_a^b K_i(r, t) \sum_{k=k_0+1}^{\infty} \frac{a_k(x+t)}{2^k}\, dt \right| \leqq 2^{-k_0} C \leqq \frac{\varepsilon}{4}. \tag{34}$$

Nach (32) kann man $r_0(k_0, \varepsilon) = r_0$ so wählen, daß für jedes $r > r_0$

$$\left| \int_a^b K_r(r, t) \sum_{k=1}^{k_0} 2^{-k} a_k(x+t) - \sum_{k=1}^{k_0} 2^{-k} a_k(x) \right| < \frac{\varepsilon}{2} \tag{35}$$

besteht. Daraus, nach (34) und (35) folgt

$$\left| \int_a^b K_r(r, t) \sum_{k=1}^{\infty} 2^{-k} a_k(x+t)\, dt - \sum_{k=1}^{\infty} 2^{-k} a_k(x) \right| < \frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \frac{\varepsilon}{4c} \leqq \varepsilon$$

für jedes $r > r_0$, womit nach (31) die Formel (33) bewiesen ist.

Es sei nun x_0 ein Punkt von N; dann ist $x_0 \in N_{k_0}$ für ein gewisses $k_0 = k_0(x_0)$ und $x_0 \in CN_k$ für alle anderen Werte von k. Für die Reihe (31) ohne das Glied mit dem Index k_0 sind alle Operationen konvergent im Punkt x_0 und für das Glied mit dem Index k_0 sind sie divergent auf N_{k_0}, insbesondere im Punkt x_0. Sie sind also divergent im Punkt x_0 für die ganze Reihe, was zu beweisen war.

Nach (20) ist die Funktion (31) beschränkt,

$$|f(x)| \leqq \sum_{k=1}^{\infty} 2^{-k} = 1,$$

überall bestimmt und die Funktionen $a_k(x)$ sind Riemann-integrabel. Laut dem Satz über gleichmäßig konvergente Reihen von Riemann-integrablen Funktionen ist die Funktion $f(x)$ selbst Riemann-integrabel.

Notwendige und hinreichende Bedingungen für die Menge N, wenn die Funktion $f(x)$ Lebesgue-integrabel ist, sind in der Arbeit [4] von Z. ZAHORSKI angegeben. Analog zu den Korollaren der Arbeit [4] folgt

Korollar I. *Bedingung* (1) *ist notwendig und hinreichend dafür, daß die Menge N gleich der Menge aller Divergenzpunkte der Summation der Fourierschen Reihe einer Riemann-integrablen Funktion ist, nach der Methode von Fejér, von Cesàro mit positiver Ordnung, oder von Abel—Poisson.*

Differentiation des bestimmten Integrals nach der oberen Grenze ist eine Operation mit einem Kern von FADDEEFF. Z. B. ist der Kern der rechtsseitigen Ableitung, $K_1(r, t)$, gleich r für $t \in \left[0, \frac{1}{r}\right]$ und gleich 0 für $t \overline{\in} \left[0, \frac{1}{r}\right]$ $(r > 0)$. Der Kern der linksseitigen Ableitung, $K_2(r, t)$, ist gleich r für $t \in \left[-\frac{1}{r}, 0\right]$, und gleich 0 für $t \overline{\in} \left[-\frac{1}{r}, 0\right]$. Endlich ist der Kern der symmetrischen Ableitung, $K_3(r, t)$, gleich $\frac{r}{2}$ für $t \in \left[-\frac{1}{r}, \frac{1}{r}\right]$, und gleich 0 für

$t \bar{\in} \left[-\frac{1}{r}, \frac{1}{r}\right]$. Der Riemann-integrablen Funktion $f(x)$ entspricht die Funktion $\varphi(x) = \int_a^x f(t)\,dt$, die die Lipschitz-Bedingung erfüllt. Es ist z. B. $\lim_{r\to\infty} \int_a^b K_3(r, t) f(x+t)\,dt = \varphi'_{\text{sym}}(x) = \lim_{h\to 0} \frac{\varphi(x+h)-\varphi(x-h)}{2h}$. Wenn wir also $n = 3$ und $R_1 = R_2 = R_3 = (0, \infty)$ setzen, so folgt:

Korollar II. *Bedingung* (1) *ist notwendig und hinreichend dafür, daß die Menge N gleich der Menge aller Nichtdifferenzierbarkeitspunkten eines bestimmten Riemannschen Integrals nach der oberen Grenze sei. Dabei kann man erreichen, daß die Funktion $\varphi(x)$ für $x \in N$ weder eine rechtsseitige oder linksseitige, noch eine symmetrische Ableitung besitzt, für $x \bar{\in} N$ aber $\varphi'(x) = f(x)$ ist.*

Literaturverzeichnis.

[1] D. K. Faddeeff, Über die Darstellung der summierbaren Funktionen in den Punkten von Lebesgue durch singuläre Integrale, *Mat. Sbornik*, **1 (43)** (1936), 351—368.
[2] F. Hausdorff, *Mengenlehre*, 2. Auflage (Berlin und Leipzig, 1927).
[3] H. Zahorska, Charakterisierung der Menge von Nichtexistenzpunkten des Randwertes harmonischer beschränkter Funktionen, *Fundamenta Math.*, **43** (1956), 338—357.
[4] Z. Zahorski, Sur les ensembles des points de divergence de certaines intégrales singulières, *Ann. de la Soc. Polonaise de Math.*, **19** (1946), 66—105.

(Eingegangen am 23. Juli 1957.)

Über die orthogonalen Funktionen. IV (Starke Summation.)

Von KÁROLY TANDORI in Szeged.

Einleitung.

Es sei $\{\varphi_n(x)\}$ ein im Intervall $[a, b]$ orthonormiertes Funktionensystem und $\{c_n\}$ eine Folge von reellen Zahlen mit $\{c_n\} \in l^2$, d. h. mit

$$\sum_{\nu=0}^{\infty} c_\nu^2 < \infty.$$

Wenn die orthogonale Reihe

$$\sum_{\nu=0}^{\infty} c_\nu \varphi_\nu(x) \tag{1}$$

im Intervall $[a, b]$ fast überall zur Funktion $f(x)$ $(C, 1)$-summierbar ist, so ist in $[a, b]$ fast überall

$$\sum_{k=0}^{N} (s_k(x) - f(x))^2 = o(N),$$

wo $s_k(x)$ die k-te Partialsumme der Reihe (1) bezeichnet:

$$s_k(x) = \sum_{\nu=0}^{k} c_\nu \varphi_\nu(x) \qquad (k = 0, 1, \ldots)$$

(siehe A. ZYGMUND [1]).

Man kann das Problem stellen, ob unter diesen Voraussetzungen die Abschätzung

$$\sum_{k=1}^{N} (s_{\nu_k}(x) - f(x))^2 = o(N) \tag{2}$$

sogar für jede Indexfolge $\nu_1 < \nu_2 < \cdots$ fast überall gilt.

Ähnliches Problem hat Z. ZALCWASSER [1] für die quadratisch-integrierbaren Fourierreihen gestellt.

Unter gewissen weiteren Annahmen bezüglich der Koeffizienten beantwortete G. ALEXITS dieses Problem positiv. Er zeigte nämlich, daß unter der weiteren Bedingung:

$$c_\nu = O\left(\frac{1}{\sqrt{\nu}\,\lambda_\nu}\right),$$

wobei $\{\lambda_\nu\}$ eine positive, monoton nichtabnehmende Folge mit monoton nichtabnehmendem $\frac{\nu}{\lambda_\nu}$ ist, für jeden Parameterwert $\alpha > \frac{1}{2}$ und für jede Indexfolge $\nu_1 < \cdots < \nu_k < \cdots$ im Intervall $[a, b]$ fast überall gilt:

$$\sum_{k=1}^{N} (\sigma_{\nu_k}^{(\alpha-1)}(x) - f(x))^2 = o(N), \tag{3}$$

wobei $\sigma_k^{(\alpha-1)}(x)$ das k-te $(C, \alpha-1)$-Mittel der Reihe (1) bezeichnet.

Für $\alpha = 1$ reduziert sich (3) auf (2).

Im Paragraphen 1 wird ein Satz bewiesen, der sich nur auf den Fall $\alpha = 1$ bezieht, jedoch für die Koeffizienten wenigere Beschränkung stellt.

Satz I. *Es sei* $\{c_\nu^*\} \in l^2$ *eine positive Zahlenfolge mit*

$$\sqrt{\nu}\, c_\nu^* \geqq \sqrt{\nu+1}\, c_{\nu+1}^* \qquad (\nu = 1, 2, \ldots) \tag{4}$$

und $\{c_\nu\}$ *eine beliebige Folge von reellen Zahlen mit*

$$c_\nu = O(c_\nu^*). \tag{5}$$

Ist die mit diesen Koeffizienten c_ν *gebildete Reihe* (1) *fast überall in* $[a, b]$ *zur Funktion* $f(x)$ $(C, 1)$*-summierbar, so besteht* (2) *für jede Indexfolge* $\nu_1 < \cdots < \nu_k < \cdots$ *fast überall in* $[a, b]$.

Da für jedes N

$$\left| \frac{s_{\nu_1}(x) + \cdots + s_{\nu_N}(x)}{N} - f(x) \right| = \left| \frac{1}{N} \sum_{k=1}^{N} (s_{\nu_k}(x) - f(x)) \right| \leqq$$

$$\leqq \sqrt{\frac{1}{N} \sum_{k=1}^{N} (s_{\nu_k}(x) - f(x))^2}$$

ist, folgt aus (2) für jede Indexfolge $\nu_1 < \cdots < \nu_k < \cdots$

$$\frac{s_{\nu_1}(x) + \cdots + s_{\nu_N}(x)}{N} \to f(x)$$

fast überall in $[a, b]$.

Im Paragraphen 2 werden wir zeigen, daß diese Behauptung im allgemeinen, ohne weitere Bedingungen bezüglich der Koeffizienten, nicht gültig ist. Es gilt nämlich der

Satz II. *Es existiert ein im Intervall* $[a, b]$ *orthonormiertes Funktionensystem* $\{\Phi_\nu(x)\}$, *eine Koeffizientenfolge* $\{c_\nu\} \in l^2$ *und eine Indexfolge* $\{\nu_k\}$ *derart, daß die Reihe*

$$\sum_{\nu=0}^{\infty} c_\nu \Phi_\nu(x) \tag{6}$$

in $[a, b]$ *fast überall zu einer quadratisch-integrierbaren Funktion* $f(x)$ $(C, 1)$-*summierbar ist und doch die Folge der Mittel*

$$\frac{S_{\nu_1}(x)+\cdots+S_{\nu_N}(x)}{N} \tag{7}$$

in $[a, b]$ *fast überall divergiert, wobei* $S_k(x)$ *die* k*-te Partialsumme der Reihe* (6) *bezeichnet. Das Funktionensystem* $\{\Phi_\nu(x)\}$ *kann in* $[a, b]$ *gleichmäßig beschränkt gewählt werden.*

Aus der Divergenz der Folge (7) folgt, daß in diesem Falle in $[a, b]$ fast überall gilt:

$$\sum_{k=1}^{N}(S_{\nu_k}(x)-f(x))^2 \neq o(N).$$

Im Paragraphen 3 werden wir noch den folgenden Satz beweisen.

Satz III. *Ist*

$$\sum_{k=2}^{\infty} c_k^2 \log k < \infty, \tag{8}$$

so gibt es eine quadratisch-integrierbare Funktion $f(x)$ *derart, daß* (2) *für jede Indexfolge* $\nu_1<\cdots<\nu_k<\cdots$ *fast überall im Intervall* $[a, b]$ *besteht.*

§ 1. Beweis von Satz I.

Es sei $\nu_1<\cdots<\nu_k<\cdots$ eine beliebige Indexfolge. Ohne Beschränkung der Allgemeinheit kann angenommen werden, daß $\nu_1 \geqq 1$. Ist $2^m \leqq \nu_k < 2^{m+1}$, so sei $\mu_k = 2^{m+1}$ $(m = 0, 1, \ldots)$. Es ist klar, daß $\mu_k \leqq 2\nu_k$ $(k = 1, 2, \ldots)$. Da nach der Annahme $\{c_\nu\} \in l^2$ ist und die Reihe (1) im Intervall $[a, b]$ fast überall zur Funktion $f(x)$ $(C, 1)$-summierbar ist, so gilt nach einem Satz von N. A. KOLMOGOROFF [1] fast überall $\lim_{m\to\infty} s_{2^m}(x) = f(x)$ und folglich

$$\lim_{k\to\infty} s_{\mu_k}(x) = f(x). \tag{1.1}$$

Für jedes N ist

$$\sum_{k=1}^{N}(s_{\nu_k}(x)-f(x))^2 \leqq 2\sum_{k=1}^{N}(s_{\nu_k}(x)-s_{\mu_k}(x))^2 + 2\sum_{k=1}^{N}(s_{\mu_k}(x)-f(x))^2. \tag{1.2}$$

Auf Grund von (1.1) ist fast überall

$$\sum_{k=1}^{N}(s_{\mu_k}(x)-f(x))^2 = o(N). \tag{1.3}$$

Nach (4) und (5) ergibt sich durch eine einfache Rechnung:

$$\sum_{k=1}^{\infty}\frac{1}{k}\int_a^b (s_{\nu_k}(x)-s_{\mu_k}(x))^2dx = O(1)\sum_{k=1}^{\infty}\frac{1}{k}\left((c^*_{\nu_k+1})^2+\cdots+(c^*_{\mu_k})^2\right)=$$

$$=O(1)\sum_{k=1}^{\infty}\frac{\mu_k-\nu_k}{k}\,\frac{(\nu_k+1)(c^*_{\nu_k+1})^2}{\nu_k+1}=O(1)\sum_{k=1}^{\infty}\frac{k(c_k^*)^2}{k}=O(1)\sum_{k=1}^{\infty}(c_k^*)^2<\infty,$$

woraus wir mit Anwendung des B. Levischen Satzes erhalten, daß die Reihe

$$\sum_{k=1}^{\infty}\frac{1}{k}(s_{\nu_k}(x)-s_{\mu_k}(x))^2$$

fast überall konvergiert. Daraus folgt mit Anwendung des bekannten Kroneckerschen Lemmas (siehe z. B. A. ZYGMUND [2], 255), daß fast überall

$$\sum_{k=1}^{N}(s_{\nu_k}(x)-s_{\mu_k}(x))^2=o(N)$$

ist. Nun ergibt sich nach (1. 2) und (1. 3), daß (2) im Intervall $[a, b]$ fast überall besteht.

Damit ist der Satz I vollständig bewiesen.

§ 2. Beweis von Satz II.

Zum Beweis von Satz II benötigen wir den folgenden Hilfssatz.

Hilfssatz. *Ist* $\{c_\nu\}\in l^2$, *so gilt für jede Indexfolge* $\nu_1<\cdots<\nu_k<\cdots$

$$\lim_{N\to\infty}\left(s_{\nu_{2^N}}(x)-\frac{1}{2^N}\sum_{k=1}^{2^N}s_{\nu_k}(x)\right)=0$$

im Grundintervall $[a, b]$ *fast überall; hier bezeichnet* $s_k(x)$ *die k-te Partialsumme der Reihe* (1).

Beweis. Durch eine einfache Rechnung ergibt sich:

$$\sum_{n=0}^{\infty}\int_a^b\left(s_{\nu_{2^n}}(x)-\frac{1}{2^n}\sum_{k=1}^{2^n}s_{\nu_k}(x)\right)^2dx=\sum_{n=1}^{\infty}\sum_{k=1}^{2^n-1}\frac{k^2}{2^{2n}}\sum_{\nu=\nu_k+1}^{\nu_{k+1}}c_\nu^2=$$

$$=\sum_{k=1}^{\infty}k^2\sum_{\nu=\nu_k+1}^{\nu_{k+1}}c_\nu^2\sum_{2^n>k}\frac{1}{2^{2n}}=O(1)\sum_{\nu=\nu_1+1}^{\infty}c_\nu^2<\infty,$$

woraus wir mit Anwendung des B. Levischen Satzes erhalten, daß die Reihe

$$\sum_{n=0}^{\infty}\left(s_{\nu_{2^n}}(x)-\frac{1}{2^n}\sum_{k=1}^{2^n}s_{\nu_k}(x)\right)^2$$

in $[a, b]$ fast überall konvergiert.

Damit haben wir also noch mehr als die Behauptung des Hilfssatzes bewiesen.

Nun gehen wir zum Beweis von Satz II über. Es sei $a_n = \frac{1}{\sqrt{n \log^3 n}}$ für $n \geqq 2$ und $a_0 = a_1 = 1$. Die Koeffizientenfolge $\{a_n\}$ ist positiv, monoton nichtwachsend und

$$\sum_{n=2}^{\infty} a_n^2 (\log n)^2 = \infty .$$

Nach einem in Mitteilung I bewiesenen Satz (K. TANDORI [1], Satz I) folgt hieraus, daß ein im Intervall $[a, b]$ orthonormiertes Funktionensystem $\{\psi_n(x)\}$ existiert, für welches die Reihe

$$\sum_{n=0}^{\infty} a_n \psi_n(x) \tag{2. 1}$$

in $[a, b]$ überall divergiert. Das Funktionensystem $\{\psi_n(x)\}$ kann sogar gleichmäßig beschränkt gewählt werden. Weiterhin ist

$$\sum_{n=4}^{\infty} a_n^2 (\log \log n)^2 < \infty \tag{2. 2}$$

und so folgt nach einem bekannten Satz (siehe D. MENCHOFF [1]), daß die Reihe (2. 1) in $[a, b]$ fast überall $(C, 1)$-summierbar ist.

Das Funktionensystem $\{\psi_n(x)\}$ kann so konstruiert werden, daß wenn man für eine geeigneterweise gewählte Indexfolge $\{N_m\}$ die $(N_m - 1)$-ten Glieder der Reihe (2. 1) wegläßt, die erhaltene Reihe in $[a, b]$ noch überall divergiert (siehe Mitteilung I, §§ 1, 2 und S. 107). Es sei die so erhaltene Reihe

$$\sum_{n=0}^{\infty} a_n^* \psi_n^*(x). \tag{2. 3}$$

Nach den obigen divergiert diese Reihe in $[a, b]$ überall. Die k-te Partialsumme der Reihe (2. 3) bezeichnen wir mit $S_k^*(x)$. Da

$$\sum_{n=4}^{\infty} (a_n^*)^2 (\log \log n)^2 < \infty \tag{2. 4}$$

ist, so folgt nach dem erwähnten Satz von D. MENCHOFF, daß die Reihe (2. 3) in $[a, b]$ fast überall zu einer quadratisch-integrierbaren Funktion $f(x)$ $(C, 1)$-summierbar ist. Nach (2. 4) ist $\{a_n^*\} \in l^2$ und so ergibt sich nach dem erwähnten Satz von A. N. KOLMOGOROFF, daß

$$\lim_{n \to \infty} S_{2^n}^*(x) = f(x) \tag{2. 5}$$

in $[a, b]$ fast überall gilt.

Nun werden wir zuerst eine Indexfolge $\nu_1<\cdots<\nu_k<\cdots$ und eine Folge von natürlichen Zahlen $M_1<\cdots<M_l<\cdots$ definieren, für welche die Bedingung

$$2^{M_l}<\nu_k<2^{M_l+1} \qquad (2^{2^l}<k\leqq 2^{2^{l+1}}) \tag{2.6}$$

bei jedem $l\geqq 1$ erfüllt wird.

Es sei $\nu_i=i$ für $i=1,\ldots,2^2$. Es sei M_1 die kleinste natürliche Zahl, für welche

$$\nu_{2^2}<2^{M_1} \quad \text{und} \quad 2^4<2^{M_1}$$

bestehen und wir nehmen $\nu_{2^2+i}=2^{M_1}+i$ für $i=1,\ldots,2^4-2^2$. Offensichtlich erfüllt sich (2.6) für $l=1$.

Es sei $\lambda(\geqq 2)$ eine beliebige natürliche Zahl. Nehmen wir an, daß die Indizes $\nu_1<\cdots<\nu_{2^{2^\lambda}}$ und die natürlichen Zahlen $M_1<\cdots<M_{\lambda-1}$ bereits so definiert sind, daß die Bedingung (2.6) für $l=1,\ldots,\lambda-1$ erfüllt wird. Es sei M_λ die kleinste natürliche Zahl, für welche

$$\nu_{2^{2^\lambda}}<2^{M_\lambda} \quad \text{und} \quad 2^{2^{\lambda+1}}<2^{M_\lambda}$$

bestehen. Es sei $\nu_{2^{2^\lambda}+i}=2^{M_\lambda}+i$ für $i=1,2,\ldots,2^{2^{\lambda+1}}-2^{2^\lambda}$. Offensichtlich ist $\nu_1<\cdots<\nu_{2^{2^{\lambda+1}}}$, $M_1<\cdots<M_\lambda$ und wird (2.6) auch für $l=\lambda$ erfüllt. Mit vollständiger Induktion erhalten wir solche Folgen $\{\nu_k\}$ und $\{M_l\}$, daß die Bedingung (2.6) für jedes l erfüllt wird.

Es sei $c_{\nu_{2^n}}=a_n^*$, $\Phi_{\nu_{2^n}}(x)=\psi_n^*(x)$ $(n=0,1,\ldots)$ und $c_\nu=0$ für $\nu\neq\nu_{2^n}$ $(n=0,1,\ldots)$. Wir bezeichnen ferner die Funktionen $\psi_{N_1}(x),\ldots,\psi_{N_m}(x),\ldots$ der Reihe nach mit $\Phi_\nu(x)$ für $\nu\neq\nu_{2^n}$ $(n=0,1,\ldots)$.

Offensichtlich ist das so erhaltene Funktionensystem $\{\Phi_n(x)\}$ in $[a,b]$ orthonormiert und gleichmäßig beschränkt, wenn das Funktionensystem $\{\psi_\nu(x)\}$ gleichmäßig beschränkt war. Nach (2.6) und nach der Konstruktion gilt es für $M_l<m\leqq M_{l+1}$

$$S_{2^m}(x)=S_{2^{l+1}}^*(x),$$

wo $S_k(x)$ die k-te Partialsumme der Reihe

$$\sum_{\nu=0}^{\infty} c_\nu \Phi_\nu(x)$$

bezeichnet. So ergibt sich aus (2.5), daß in $[a,b]$ fast überall

$$\lim_{m\to\infty} S_{2^m}(x)=f(x)$$

gilt. Da $\{c_\nu\}\in l^2$ ist, so folgt nach einem bekannten Satz (siehe S. KACZMARZ [1]), daß die Reihe (2.7) in $[a,b]$ fast überall zur quadratisch-integrierbaren Funktion $f(x)$ $(C,1)$-summierbar ist.

Nach der Konstruktion ist weiterhin klar, daß $S_{\nu_{2^N}}(x) = S_N^*(x)$ $(N=0,1,\ldots)$ ist und so divergiert die Folge $\{S_{\nu_{2^N}}(x)\}$ in $[a,b]$ überall. Daraus erhalten wir mit Anwendung unseres Hilfssatzes, daß die Folge

$$\frac{S_{\nu_1}(x)+\cdots+S_{\nu_N}(x)}{N}$$

in $[a,b]$ fast überall divergiert.

Also erfüllen die Folgen $\{c_\nu\}$, $\{\nu_k\}$ und das Funktionensystem $\{\Phi_\nu(x)\}$ alle im Satz II stehenden Bedingungen.

Damit haben wir Satz II vollständig bewiesen.

§ 3. Beweis von Satz III.

Ist die Bedingung (8) erfüllt, so folgt nach einem bekannten Satz (D. MENCHOFF [1]), daß die Reihe (1) fast überall in $[a,b]$ zu einer quadratisch integrierbaren Funktion $f(x)$ $(C,1)$-summierbar ist. So besteht nach einem anderen bekannten Satz (A. N. KOLMOGOROFF [1]) $\lim_{n\to\infty} s_{2^n}(x) = f(x)$ fast überall in $[a,b]$. Es sei $\mu_n = 2^m$ für $2^m \leqq \nu_n < 2^{m+1}$ $(m=0,1,\ldots)$. Dann ist $\lim_{n\to\infty} s_{\mu_n}(x) = f(x)$ und folglich

$$\sum_{n=1}^{N} (s_{\mu_n}(x)-f(x))^2 = o(N) \tag{3.1}$$

fast überall in $[a,b]$.

Nun ist

$$\sum_{n=1}^{N} (s_{\nu_n}(x)-f(x))^2 \leqq 2\sum_{n=1}^{N} (s_{\nu_n}(x)-s_{\mu_n}(x))^2 + 2\sum_{n=1}^{N} (s_{\mu_n}(x)-f(x))^2. \tag{3.2}$$

Mit einfacher Rechnung bekommen wir auf Grund der Annahme (8):

$$\sum_{n=2}^{\infty} \frac{1}{n}\int_a^b (s_{\nu_n}(x)-s_{\mu_n}(x))^2\,dx = \sum_{n=2}^{\infty} \frac{1}{n}(c^2_{\mu_n+1}+\cdots+c^2_{\nu_n}) \leqq$$

$$\leqq \sum_{m=0}^{\infty} \sum_{k=2^m+1}^{2^{m+1}} c_k^2 \sum_{2^m<\nu_n\leqq 2^{m+1}} \frac{1}{n} \leqq \sum_{m=0}^{\infty} \sum_{k=2^m+1}^{2^{m+1}} c_k^2 \sum_{l=1}^{2^m} \frac{1}{l} \leqq$$

$$\leqq \sum_{m=0}^{\infty} \sum_{k=2^m+1}^{2^{m+1}} c_k^2 \sum_{l=1}^{k} \frac{1}{l} \leqq \sum_{k=1}^{\infty} c_k^2(1+\log k) < \infty$$

und so ergibt sich mit Anwendung des B. Levischen Satzes, daß die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n}(s_{\nu_n}(x)-s_{\mu_n}(x))^2$$

in $[a, b]$ fast überall konvergiert. Daraus folgt mit Anwendung des Kroneckerschen Lemmas, daß

$$\sum_{n=1}^{N} (s_{\nu_n}(x) - s_{\mu_n}(x))^2 = o(N)$$

in $[a, b]$ fast überall gilt. Daraus, auf Grund von (3. 1) und (3. 2) ergibt sich die Behauptung.

Damit haben wir Satz III bewiesen.

Schriftenverzeichnis.

Alexits, G., [1] Eine Bemerkung zur starken Summierbarkeit der Orthogonalreihen, *Acta Sci. Math.*, **16** (1955), 127—129.

Kolmogoroff, A. N., [1] Une contribution à l'étude de la convergence des séries de Fourier, *Fundamenta Math.*, **5** (1924), 96—97.

Menchoff, D., [1] Sur les séries de fonctions orthogonales (Deuxième Partie), *Fundamenta Math.*, **8** (1926), 56—108.

Tandori, K., [1] Über die orthogonalen Funktionen. I, *Acta Sci. Math.*, **18** (1957), 57—130.

Zalcwasser, Z., [1] Sur la sommabilité des séries de Fourier, *Studia Math.*, **6** (1936), 82—88.

Zygmund, A., [1] Sur l'applications de la première moyenne arithmétique dans la théorie des séries de fonctions orthogonales, *Fundamenta Math.*, **10** (1927), 356—362; [2] *Trigonometrical series* (Warszawa—Lwów, 1935).

(Eingegangen am 2. Oktober 1957.)

Sur les contractions de l'espace de Hilbert. III.

Par BÉLA SZ.-NAGY à Szeged et CIPRIAN FOIAŞ à Bucarest.

A la mémoire de J. von Neumann.

Dans cet article on traitera des relations spectrales et fonctionnelles entre les contractions de l'espace de Hilbert et les transformations unitaires qui leur correspondent dans le sens des articles précédents du premier auteur, ainsi que des relations entre semi-groupes de contractions et leurs "génératrices" et "cogénératrices". Faisant usage de la notion de l'ensemble spectral, due à J. VON NEUMANN, on passe ensuite du cas d'une contraction et du disque unité du plan complexe au cas d'une transformation linéaire bornée quelconque T et d'un ensemble spectral de T.

I.

1. Soit T une contraction de l'espace de Hilbert $\mathfrak{H}$. On sait (voir [10], [11], [13]) qu'il existe, dans un espace de Hilbert $\mathfrak{K} \supseteq \mathfrak{H}$, une transformation unitaire U telle qu'on ait

$$T^n = \mathrm{pr}\, U^n \qquad (n = 0, 1, 2, \ldots)^1)$$

et que $\mathfrak{K}$ soit sous-tendu par les éléments de la forme $U^n h$ ($h \in \mathfrak{H}$; $n = 0, \pm 1, \pm 2, \ldots$); ces conditions déterminent U d'une manière univoque[2]); appelons U *la dilatation unitaire* de la contraction T.

Le théorème suivant établit une relation spectrale simple entre T et U.

Théorème 1. *Si U est la dilatation unitaire de la contraction T, toute valeur propre de T de module 1 est une valeur propre de U aussi et inversement. Les vecteurs propres correspondants sont les mêmes pour T et U.*

Démonstration. La dilatation unitaire de cT ($|c| = 1$) étant évidemment égale à cU, il suffit d'envisager le cas de la valeur propre 1. Ce qu'il

---

1) Nous utilisons la terminologie de [12] et [13].

2) A condition qu'on ne distingue pas entre les différentes réalisations du prolongement $\mathfrak{K}$ de $\mathfrak{H}$.

faut alors démontrer c'est que (i) $Th=h$ pour un $h\in\mathfrak{H}$ entraîne $Uh=h$, (ii) $Uf=f$ pour un $f\in\mathfrak{K}$ entraîne $f\in\mathfrak{H}$ et $Tf=f$.

Ad (i): $Th=h$ entraîne $\|Uh\|=\|h\|=\|Th\|$; or comme on a $Th=PUh$ où P est la projection orthogonale de $\mathfrak{K}$ sur $\mathfrak{H}$, cela entraîne que $Uh=Th$, donc $Uh=h$.

Ad (ii): Soit $Uf=f$, $f\in\mathfrak{K}$. L'espace $\mathfrak{K}$ étant sous-tendu par les éléments de la forme $U^n h$ ($h\in\mathfrak{H}$; $n=0,\pm1,\pm2,\ldots$), f peut être représenté sous la forme

$$f=\lim f_n \quad \text{où} \quad f_n=\sum_{k=-r_n}^{r_n} U^k h_{n,k},\ h_{n,k}\in\mathfrak{H}.$$

Vu que $U^r f=f$ pour tout entier r, on a pour $n\to\infty$

$$\|U^{r_n} f_n-f\|=\|U^{r_n}(f_n-f)\|=\|f_n-f\|\to 0,$$

donc

$$\sum_{m=0}^{2r_n} U^m g_{n,m}\to f \quad \text{où} \quad g_{n,m}=h_{n,m-r_n},$$

et par conséquent

$$\sum_{m=0}^{2r_n} U^{m+1} g_{n,m}\to Uf=f.$$

En appliquant la projection P il en résulte que

$$u_n=\sum_{m=0}^{2r_n} T^m g_{n,m}\to Pf, \quad Tu_n=\sum_{m=0}^{2r_n} T^{m+1} g_{n,m}\to Pf,$$

donc

$$TPf=Pf. \tag{1}$$

En vertu de la proposition (i), déjà démontrée, il s'ensuit que

$$UPf=Pf,$$

et comme on a par hypothèse $Uf=f$, il résulte que

$$U(I-P)f=(I-P)f, \quad \text{donc aussi} \quad U^m(I-P)f=(I-P)f \quad (m=0,\pm1,\pm2,\ldots).$$

Or $(I-P)f$ est orthogonal à $\mathfrak{H}$ et alors $U^m(I-P)f$ est orthogonal à $U^m\mathfrak{H}$, et de cette façon $(I-P)f$ est orthogonal à tous les sous-espaces $U^m\mathfrak{H}$, ce qui n'est possible que si $(I-P)f=0$. Donc $f=Pf\in\mathfrak{H}$; en vertu de (1) cela achève la démonstration.

2. Passons au calcul fonctionnel avec la contraction T. Convenons d'abord d'une définition:

Définition 1. *Soit $\mathcal{O}(S_0)$ la classe des fonctions $u(\lambda)$, holomorphes dans un domaine du plan complexe contenant le disque unité fermé*

$$S_0 = \{\lambda : |\lambda| \leqq 1\}$$

(ce domaine pouvant varier avec u).

On définit par la formule

$$u(\lambda) = \sum_{n=0}^{\infty} c_n \lambda^n \to \sum_{n=0}^{\infty} c_n T^n = u(T) \tag{2}$$

une application de la classe $\mathcal{O}(S_0)$ dans l'algèbre des transformations linéaires bornées de l'espace $\mathfrak{H}$ (la série des transformations converge en norme puisque $\limsup |c_n|^{\frac{1}{n}} < 1$ et $\|T\| \leqq 1$). Cette application est évidemment linéaire et multiplicative:

$$(c_1 u_1 + c_2 u_2)(T) = c_1 u_1(T) + c_2 u_2(T), \quad (u_1, u_2)(T) = u_1(T)\, u_2(T);$$

de plus on a, vu que la projection est une transformation linéaire continue,

$$u(T) = \mathrm{pr}\, u(U) \tag{3}$$

où U est la dilatation unitaire de T.

Or cette formule nous offre une possibilité d'étendre la classe des fonctions envisagées, en effet, $u(U)$ a sens pour des fonctions $u(\lambda)$ de type beaucoup plus général. Notamment, si $\{E_\Theta\}$ est la famille spectrale de U $(0 \leqq \Theta \leqq 2\pi)$, $u(U)$ a sens par la formule

$$(u(U) f, g) = \int_0^{2\pi} u(e^{i\Theta})\, d(E_\Theta f, g) \qquad (f, g \in \mathfrak{H}) \tag{4}$$

pour toute fonction $u(\lambda)$ dont les valeurs sur le cercle unité constituent une fonction $u(e^{i\Theta})$, définie presque partout, bornée et mesurable par rapport à E_Θ, c'est-à-dire par rapport à chaque fonction non-décroissante $(E_\Theta f, f)$ $(f \in \mathfrak{H})$. Pour ces fonctions l'application $u(\lambda) \to u(U)$ est linéaire et multiplicative (et pour $u \in \mathcal{O}$ coïncide avec la définition par (2)), de plus on a

$$\|u(U)\| = \text{vrai max}\, |u(e^{i\Theta})|, \tag{5}$$

le vrai maximum étant considéré par rapport à E_Θ. Mais si l'on veut définir, pour toutes ces fonctions, l'application $u(\lambda) \to u(T)$ par (3), celle-ci sera bien linéaire mais en général non-multiplicative.

Cela impose le problème de choisir une sous-classe de ces fonctions formant une algèbre, pour laquelle cette application soit aussi multiplicative; cette sous-classe doit naturellement comprendre la classe $\mathcal{O}(S_0)$ et doit être fermée dans un certain sens. En ce but, donnons la définition suivante:

Définition 2. *Soit $\mathcal{C}_T(S_0)$ la classe des fonctions $u(\lambda)$, bornées et holomorphes dans l'intérieur du disque unité S_0 et pour lesquelles*

$$u(e^{i\Theta}) = \lim_{r\to 1-0} u(re^{i\Theta})$$

existe en tout point $e^{i\Theta}$ du cercle unité exceptés peut-être les points d'un ensemble dénombrable, ne contenant aucune valeur propre de T.

La fonction $u(e^{i\Theta})$ est alors définie, en vertu du théorème 1, presque partout par rapport à E_Θ, et est bornée et mesurable par rapport à E_Θ, donc $u(U)$ et $u(T)$ existent, *définies par les formules* (3) *et* (4).

La classe $\mathcal{C}_T(S_0)$ est évidemment une algèbre et contient la classe $\mathcal{C}(S_0)$ comme une sous-algèbre. On a le

Théorème 2. (i) *L'application $u(\lambda)\to u(T)$, définie pour la classe $\mathcal{C}_T(S_0)$ par les formules* (3) *et* (4), *est linéaire, multiplicative, et telle que*

$$\|u(T)\| \leqq \sup_{|\lambda|<1} |u(\lambda)|. \tag{6}$$

Pour $u(\lambda)\in\mathcal{C}(S_0)$ cette définition est équivalente à la définition directe (2).

(ii) *Pour toute suite $u_n(\lambda)\in\mathcal{C}_T(S_0)$, tendant vers $u(\lambda)\in\mathcal{C}_T(S_0)$ dans le sens que $u_n(\lambda)$ est également bornée dans l'intérieur de S_0 et $u_n(e^{i\Theta})$ tend vers $u(e^{i\Theta})$ en tout point $e^{i\Theta}$ exceptés peut-être les points d'un ensemble dénombrable ne contenant aucune valeur propre de T, on a*

$$u_n(T)\to u(T) \qquad \text{(convergence forte).}$$

(iii) *Pour T normale et $u(\lambda)\in\mathcal{C}_T(S_0)$ la définition de $u(T)$ par* (3) *et* (4) *est équivalente à la définition usuelle moyennant la décomposition spectrale $T=\int\lambda dK_\lambda$; on a notamment*

$$(u(T)f,g)=\int u(\lambda)\,d(K_\lambda f,g), \quad \|u(T)f\|^2=\int|u(\lambda)|^2\,d\|K_\lambda f\|^2, \tag{7}$$

l'intégration étant étendue sur le spectre de T (qui est contenu dans le disque S_0).

(iv) *Soit $\lambda\to l(\lambda)$ une application homographique du disque unité S_0 sur lui-même, $l(\lambda)=a(\lambda-b)(1-\bar b\lambda)^{-1}$ ($|a|=1$, $|b|<1$); on a alors $l(\lambda)\in\mathcal{C}(S_0)$ et $T'=l(T)$ est une contraction. Pour toute fonction $u(\lambda')\in\mathcal{C}_{T'}(S_0)$ la fonction composée $u\circ l(\lambda)=u(l(\lambda))$ appartient à $\mathcal{C}_T(S_0)$ et on a*

$$u\circ l(T)=u(T').$$

(v) *Pour $u(\lambda)\in\mathcal{C}_T(S_0)$ le spectre de la transformation $T'=u(T)$ est contenu dans l'adhérence $\bar Z$ de l'ensemble Z (évidemment borné) des valeurs de la fonction $u(\lambda)$ prises dans l'intérieur de S_0. Pour toute fonction $w(z)$,*

holomorphe dans un domaine E_w du plan complexe contenant l'ensemble $\bar{Z}$ dans son intérieur, $w \circ u(\lambda) = w(u(\lambda))$ appartient à $\mathcal{O}_T(S_0)$ et on a

$$w \circ u(T) = w^R(u(T))$$

où $w^R(T')$ désigne la transformation qui correspond à la fonction $w(z)$ et à la transformation T' par le calcul fonctionnel de Riesz—Dunford (cf. [7] n° 151).

Démonstration. Sauf l'assertion concernant la multiplicativité, (i) découle immédiatement de la définition et de (5) si l'on remarque que

$$\sup|u(e^{i\Theta})| \leqq \sup_{|\lambda|<1} |u(\lambda)|.$$

(ii) découle du théorème de convergence de Lebesgue; en effet, on a

$$\|[u_n(T)-u(T)]f\|^2 \leqq \|[u_n(U)-u(U)]f\|^2 = \int_0^{2\pi} |u_n(e^{i\Theta})-u(e^{i\Theta})|^2 \, d\|E_\Theta f\|^2,$$

or les fonctions sous le signe d'intégrale sont également bornées et tendent vers 0 pour $n \to \infty$, presque partout par rapport à E_Θ.

Pour $u(\lambda) \in \mathcal{O}_T(S_0)$ on a $u_r(\lambda) = u(r\lambda) \in \mathcal{O}(S_0)$ $(0 < r < 1)$, et lorsque $r \to 1-0$, $u_r(\lambda)$ tend vers $u(\lambda)$ dans le sens de (ii). Donc on a

$$u_r(T) \to u(T) \qquad \text{(convergence forte).} \tag{8}$$

Grâce à la propriété multiplicative de l'application pour la classe $\mathcal{O}(S_0)$, il s'ensuit que si $u, v \in \mathcal{O}_T(S_0)$, on a d'une part

$$(uv)_r(T) = u_r(T)\, v_r(T) \to u(T)\, v(T);$$

d'autre part

$$(uv)_r(T) \to (uv)(T),$$

donc $(uv)(T) = u(T)\, v(T)$, ce qui prouve la propriété multiplicative pour la classe $\mathcal{O}_T(S_0)$.

Si T est normale et $u(\lambda) \in \mathcal{O}(S_0)$, la définition de $u(T)$ par (3), (4) est équivalente à la définition par (2), et celle-ci est équivalente à la définition par (7), donc, dans ce cas, la définition par (3), (4) est équivalente à la définition par (7). On en passe au cas d'une fonction $u(\lambda) \in \mathcal{O}_T(S_0)$ en faisant intervenir de nouveau les fonctions $u_r(\lambda)$ et en remarquant que, en vertu du théorème de convergence de Lebesgue,

$$\int u_r(\lambda)\, d(K_\lambda f, g) \to \int u(\lambda)\, d(K_\lambda f, g) \qquad (r \to 1-0).$$

Cela prouve (iii)

Prouvons (iv). Le fait que $l(\lambda) \in \mathcal{O}(S_0)$ est immédiat, donc T' existe; $\|T'\| \leqq 1$ s'ensuit de (6). En vertu des relations $T' = a(T-b)(I-\bar{b}T)^{-1}$, $T = \bar{a}(T'+abI)(I+\bar{a}\bar{b}T')^{-1}$, les valeurs propres de T' sont précisément les images des valeurs propres de T par l'application $\lambda \to l(\lambda)$. Par (i) on a $l^n(T) = [l(T)]^n$ et plus généralement $p \circ l(T) = p(T')$ pour tout polynome

$p(\lambda)$; (8) en dérive pour tout $u \in \mathcal{O}(S_0)$ par (ii), parce que les sommes partielles $p_n(\lambda)$ de la série entière de $u(\lambda)$ convergent uniformément vers $u(\lambda)$ sur le cercle $|\lambda| = 1$, de même que les $p_n \circ l(\lambda)$ vers $u \circ l(\lambda)$. Dans le cas général d'une fonction $u(\lambda) \in \mathcal{O}_T(S_0)$ envisageons les fonctions $u_r(\lambda) \in \mathcal{O}(S_0)$. Remarquons tout d'abord que, pour $r \to 1-0$,

$$\lim u(rl(e^{i\Theta})) = \lim u(l(re^{i\Theta}))$$

en tout point $e^{i\Theta}$ où la première limite existe; en effet, la valeur limite de $u(\lambda)$ en un point λ_0 du cercle unité est la même si le point variable λ ($|\lambda| < 1$) s'approche de λ_0 le long du rayon ou le long d'un cercle orthogonal au cercle unité (ou le long de n'importe quel chemin qui reste dans un angle formé par deux cordes du cercle unité issues de λ_0). De là il s'ensuit que pour $r \to 1-0$ la limite de $u \circ l(re^{i\Theta})$ existe en tout point $e^{i\Theta}$ avec peut-être un ensemble dénombrable d'exceptions, elle existe en particulier en tout point $e^{i\Theta}$ pour lequel $l(e^{i\Theta})$ est une valeur propre de T', c'est-à-dire pour lequel $e^{i\Theta}$ lui-même est une valeur propre de T. Cela veut dire que $u \circ l(\lambda) \in \mathcal{O}_T(S_0)$. La relation $u_r \circ l(T) = u_r(T')$ étant vraie pour tout r ($0 < r < 1$), la relation $u \circ l(T) = u(T')$ s'ensuit par (ii). En effet, lorsque r tend vers $1-0$, $u_r(\lambda)$ tend vers $u(\lambda)$ dans le sens de (ii) par rapport à T', et $u_r \circ l(\lambda) = u(rl(\lambda))$ tend vers $u(l(\lambda)) = u \circ l(\lambda)$ dans le sens de (ii) par rapport à T.

Reste à prouver (v). Pour $z \notin \bar{Z}$ la fonction $v_z(\lambda) = [z - u(\lambda)]^{-1}$ appartient évidemment à $\mathcal{O}_T(S_0)$, et grâce à la propriété multiplicative on a $v_z(T) = [zI - u(T)]^{-1}$. Cela prouve que z n'appartient pas au spectre $\sigma(T')$ de $T' = u(T)$, donc $\sigma(T') \subseteq \bar{Z}$. Soit alors $w(z)$ une fonction, holomorphe dans un domaine (ouvert connexe) E_w contenant l'ensemble $\bar{Z}$ dans son intérieur. Puisque $\bar{Z}$ est borné, fermé (et connexe) il existe un domaine D tel que $\bar{Z} \subset D \subset E_w$ et dont la frontière ∂D se compose d'un nombre fini de courbes fermées jordaniennes rectifiables C_k passant dans E_w et orientées conformément à l'orientation de D comme sous-ensemble ouvert du plan complexe orienté (l'existence de tel domaine D peut être démontrée par application du théorème de recouvrement de Borel). Soit d (> 0) la distance de ∂D à $\bar{Z}$. Envisageons une décomposition de chaque C_k par des points consécutifs $z_0^{(k)}, z_1^{(k)}, \ldots, z_{n_k}^{(k)} = z_0^{(k)}$ et y faisons correspondre la fonction

$$s(\lambda) = \frac{1}{2\pi i} \sum_k \sum_{n=1}^{n_k} \frac{w(z_n^{(k)})}{z_n^{(k)} - u(\lambda)} (z_n^{(k)} - z_{n-1}^{(k)}).$$

Celle-ci est holomorphe dans l'intérieur de S_0 et y est bornée par une constante indépendante de la décomposition particulière choisie:

$$|s(\lambda)| \leqq \frac{1}{2\pi} \max_{z \in \partial D} |w(z)| \cdot \frac{1}{d} \cdot |\partial D|$$

où $|\partial D|$ désigne la longueur totale de ∂D. La limite radiale $s(e^{i\Theta})$ existe en tout point où celle de $u(\lambda)$ existe. Donc $s(\lambda) \in \mathcal{C}_T(S_0)$. Faisons varier les décompositions des courbes C_k de sorte qu'elles deviennent infiniment fines, $s(\lambda)$ tend alors vers la fonction

$$\frac{1}{2\pi i}\int_{\partial D}\frac{w(z)}{z-u(\lambda)}\,dz = w(u(\lambda)) = w \circ u(\lambda)$$

au sens de (ii), et par conséquent $s(T)$ tend vers $w \circ u(T)$. D'autre part il découle de (i) et de la définition de $w^{\mathrm{R}}(u(T))$:

$$s(T) = \frac{1}{2\pi i}\sum_k \sum_{n-1}^{n_k} w(z_n^{(k)})[z_n^{(k)} I - u(T)]^{-1}(z_n^{(k)} - z_{n-1}^{(k)}) \to$$

$$\to \frac{1}{2\pi i}\int_{\partial D} w(z)[zI - u(T)]^{-1}\,dz = w^{\mathrm{R}}(u(T)).$$

Cela achève la démonstration.

Corollaire 2.1. *Si $T \subseteq U$, c'est-à-dire si T est isométrique, on a $u(T) \subseteq u(U)$ pour toute fonction $u(\lambda) \in \mathcal{C}_T(S_0)$.* [3])

Démonstration. Pour $u(\lambda) \in \mathcal{C}(S_0)$ cela découle de (2). On en passe aux fonctions $u(\lambda) \in \mathcal{C}_T(S_0)$ par l'intermédiaire des fonctions $u_r(\lambda) \in \mathcal{C}(S_0)$ faisant usage de (8).

Corollaire 2.2. *Si la contraction T n'est pas unitaire, le spectre de sa dilatation unitaire U recouvre le cercle unité.*

Démonstration. En cas contraire il y a un arc fermé α du cercle unité (différent du cercle entier) portant tout le spectre de U; comme α est à l'intérieur d'un domaine simplement connexe du plan complexe ne contenant pas le point 0, il s'ensuit du théorème de RUNGE qu'il existe une suite de polynomes $p_n(\lambda)$ tendant uniformément vers la fonction $1/\lambda$ sur α. En vertu de (5) on a alors

$$\|U^{-1} - p_n(U)\| \leqq \max_{\lambda \in \alpha} |1/\lambda - p_n(\lambda)| \to 0 \qquad (n \to \infty),$$

donc

$$p_n(U) \to U^{-1}, \quad Up_n(U) \to I_{\mathfrak{M}} \text{ (transformation identique de } \mathfrak{R}),$$

et par conséquent

$$p_n(T) = \mathrm{pr}\, p_n(U) \to \mathrm{pr}\, U^{-1} = \mathrm{pr}\, U^* = T^*, \quad Tp_n(T) = \mathrm{pr}\, Up_n(U) \to I.$$

---

[3]) Pour les transformations isométriques un calcul fonctionnel voisin a été proposé (implicitement) par PLESSNER [5], [6].

Il s'ensuit que

$$T^* T = [\lim p_n(T)]\, T = \lim [p_n(T)\, T] = I,$$
$$T T^* = T \lim p_n(T) = \lim [T p_n(T)] = I.$$

Donc $T^* T = T T^* = I$, T est unitaire.

II.

3. Indiquons maintenant quelques applications de ce calcul fonctionnel aux semi-groupes à un paramètre $\{T_s\}_{s \geqq 0}$ de contractions de l'espace de Hilbert $\mathfrak{H}$, continus dans le sens que $T_s \to I$ pour $s \to 0$. On sait que la transformation „infinitésimale"

$$A = \lim_{s \to 0} \frac{1}{s} (T_s - I) \tag{9}$$

est linéaire, fermée, à domaine dense dans $\mathfrak{H}$, $A - I$ admet une inverse partout définie et bornée, et la transformation

$$T = (A + I)(A - I)^{-1} \tag{10}$$

est une contraction; inversement pour toute transformation A jouissant de ces propriétés il existe un semi-groupe de contractions continu $\{T_s\}$ et un seul tel que la relation (9) soit vérifiée[4]). On appellera A la *génératrice* du semi-groupe $\{T_s\}$.

La contraction T n'a pas la valeur propre 1; en effet, comme on a $T = I + 2(A - I)^{-1}$, $Th = h$ entraîne $(A - I)^{-1} h = 0$, $h = 0$. Inversement, pour toute contraction T dont 1 n'est pas une valeur propre, il existe une transformation A et une seule avec laquelle T soit en relation (10), notamment $A = (T + I)(T - I)^{-1} = I + 2(T - I)^{-1}$.[5])

Donc, pour toute contraction T n'ayant pas la valeur propre 1, il existe un semi-groupe continu de contractions $\{T_s\}$ et un seul tel que les relations (9) et (10) soient vérifiées. Appelons T la *cogénératrice* de $\{T_s\}$.

La relation mutuelle entre le semi-groupe $\{T_s\}$ et sa cogénératrice T est explicitée par le théorème suivant:

Théorème 3. *On a pour tout* $s \geqq 0$

$$T_s = u_s(T) \quad \text{où} \quad u_s(\lambda) = \exp\left(s \frac{\lambda + 1}{\lambda - 1}\right), \tag{11}$$

et inversement

$$R_s = [T_s - (1 - s) I]\, [T_s - (1 + s) I]^{-1} \to T \qquad (s \to 0). \tag{12}$$

---

[4]) Théorème de Hille et Yosida, cf. [2] p. 238, adapté aux semi-groupes de contractions de l'espace de Hilbert, cf. [12] p. 6—8 ou [1] § 5.

[5]) $(T - I)^{-1}$ a son domaine dense dans $\mathfrak{H}$, puisque en cas contraire 1 serait une valeur propre de T^* et alors de T aussi, cf. [10] ou [13] § 4.3.

Démonstration. La fonction $u_s(\lambda)$ a son seul point singulier $\lambda=1$, et pour $|\lambda|\leqq 1$, $\lambda\neq 1$, on a $|u_s(\lambda)|\leqq 1$. Puisque T est une contraction n'ayant pas la valeur propre 1, on a $u_s(\lambda)\in\mathcal{O}_T(S_0)$, donc $u_s(T)$ existe et, en vertu du théorème 2 (6), $u_s(T)$ est une contraction pour tout $s\geqq 0$. De plus les relations $u_t(\lambda)\,u_s(\lambda)=u_{t+s}(\lambda)$, $\lim_{s\to 0} u_s(\lambda)=1$ $(|\lambda|\leqq 1,\ \lambda\neq 1)$ entraînent, en vertu du théorème 2, (i) et (ii), que les contractions $u_s(T)$ forment un semi-groupe continu. Soient A' et T' la génératrice et la cogénératrice de $u_s(T)$; montrons que $T'=T$.

Envisageons à cet effet les fonctions

$$v_s(\lambda)=\frac{u_s(\lambda)-1+s}{u_s(\lambda)-1-s}\qquad (s>0);$$

$v_s(\lambda)$ est holomorphe pour $|\lambda|<1$, continue pour $|\lambda|\leqq 1$, $\lambda\neq 1$, et on a $|v_s(\lambda)|\leqq 1$ et $\lim_{s\to 0} v_s(\lambda)=\lambda$ pour $|\lambda|\leqq 1$, $\lambda\neq 1$. En vertu du théorème 2, $v_s(T)$ existe et on a

$$\|v_s(T)\|\leqq 1,\qquad \lim_{s\to 0} v_s(T)=T \text{ (limite forte).} \tag{13}$$

La relation $v_s(\lambda)\,[u_s(\lambda)-1-s]=u_s(\lambda)-1+s$ entraîne, en vertu du théorème 2 (i), la relation

$$v_s(T)\,[u_s(T)-(1+s)\,I]=u_s(T)-(1-s)\,I, \tag{14}$$

d'où il s'ensuit que

$$v_s(T)=[u_s(T)-(1-s)\,I]\,[u_s(T)-(1+s)\,I]^{-1} \tag{15}$$

(l'inverse en question existe puisque $\|u_s(T)\|\leqq 1$ et $1+s>1$). D'autre part, en appliquant les transformations figurant aux deux membres de (14) à un élément h du domaine de A', divisant par s et faisant tendre ensuite s vers 0, il résulte en vertu de (13):

$$T(A'-I)\,h=(A'+I)\,h.$$

Donc on a

$$T(A'-I)=A'+I,\quad T=(A'+I)(A'-I)^{-1}$$

ce qui prouve que $T=T'$. Cela extraîne que $T_s=u_s(T)$; enfin, (13) et (15) entraînent (12).

Remarque. Ce raisonnement prouve que, pour toute contraction T n'ayant pas la valeur propre 1, on peut construire par (11) un semi-groupe de contractions $\{T_s\}$ qui est avec T en la relation exprimée par (9) et (10). *L'unicité* de tel semi-groupe résulte, comme on l'a déjà dit, du théorème de HILLE et YOSIDA.

4. Le théorème suivant, conséquence du théorème 3, montre qu'un semi-groupe de contractions et sa cogénératrice sont, pour ainsi dire, toujours de même type.

Théorème 4. *Pour que le semi-groupe continu de contractions $\{T_s\}$ soit constitué de transformations normales, autoadjointes ou unitaires, il faut et il suffit que sa cogénératrice T soit normale, autoadjointe ou unitaire, selon les cas.*

Démonstration. Si $\{T_s\}$ est constitué de transformations normales, T_s est permutable avec T_t pour tout s, t,[6]) d'où il s'ensuit que les transformations R_s, $R_s - R_t$ (voir (12)) sont aussi normales, et par conséquent $\|R_s h\| = \|R_s^* h\|$, $\|(R_s - R_t)h\| = \|(R_s^* - R_t^*)h\|$ pour tout $h \in \mathfrak{H}$. Or, d'après (12) on a $R_s \to T$ et par conséquent $R_s^* \to T^*$ pour $s \to 0$; les relations que nous venons d'obtenir entraînent que R_s^* converge vers T^* aussi fortement, et que $\|Th\| = \|T^* h\|$, donc T est aussi normale.

Si les T_s sont autoadjointes, les R_s sont de même ainsi que leur limite T. Si les T_s sont unitaires, on a

$$\|h\| \geqq \|R_s h\| \geqq \frac{2-s}{2+s}\|h\| \qquad \text{pour} \quad 0 < s \leqq 1;$$

cette inégalité découle de ce que pour $|\lambda| = 1$ on a

$$1 \geqq \left|\frac{\lambda - (1-s)}{\lambda + (1+s)}\right| \geqq \frac{2-s}{2+s}.$$[7])

Il s'ensuit que $\|Th\| = \lim_{s \to 0} \|R_s h\| = \|h\|$. Vu que T doit être normale, cela implique que T est unitaire.

Supposons maintenant que T est normale ayant la décomposition spectrale $T = \int \lambda \, dK_\lambda$.[8]) On a alors d'après (11) et (7)

$$T_s = \int u_s(\lambda)\, dK_\lambda,$$

donc les T_s sont aussi normales. Comme il suffit d'intégrer ici sur le spectre de T, et comme $u_s(\lambda)$ est de valeurs réelles sur l'axe réel et de module 1 sur le cercle unité, il s'ensuit que si T est autoadjointe ou unitaire, il en est de même de T_s, selon les cas.

Dans le cas de T_s unitaires on a donc

$$T_s = \int_{|\lambda|=1} \exp\left(s\frac{\lambda+1}{\lambda-1}\right) dK_\lambda$$

et cette représentation se réduit à celle du théorème de STONE,

$$T_s = \int_{-\infty}^{\infty} e^{isx}\, dE_x,$$

---

[6]) Cf. [9] p. 74.

[7]) Cf. le raisonnement sur la fonction $u_s(z)$ dans [12] p. 7—8.

[8]) Puisque T n'a pas la valeur propre 1, la mesure spectrale du point 1 est égale à O.

si l'on passe du cercle unité, privé du point $\lambda = 1$, à l'axe réel par l'application

$$\lambda \to x = -i\frac{\lambda+1}{\lambda-1} \qquad (|\lambda| = 1, \lambda \neq 1).^{9})$$

De même, si les T_s sont autoadjointes, on parvient à la représentation spectrale

$$T_s = \int_{-\infty}^{\infty} e^{-ty}\, dE_y,^{10})$$

et cela en passant de l'intervalle $-1 \leqq \lambda < 1$ au demi-axe $0 \leqq y < \infty$ par l'application

$$\lambda \to y = \frac{1+\lambda}{1-\lambda}.$$

5. Soit $\{T_s\}$ un semi-groupe continu de contractions de $\mathfrak{H}$, T sa cogénératrice, et U la dilatation unitaire de T, opérant dans l'espace $\mathfrak{K} \supseteq \mathfrak{H}$. Soit $\{U_s\}$ le groupe continu à un paramètre de transformations unitaires de l'espace $\mathfrak{K}$, dont la cogénératrice est égale à U. Puisqu'on a $U_s = u_s(U)$, $T_s = u_s(T)$ pour $s \geqq 0$, on a par la définition même de $u_s(T)$:

$$T_s = \operatorname{pr} U_s \qquad (s \geqq 0). \tag{16}$$

Montrons que l'espace $\mathfrak{K}$ est sous-tendu par les éléments de la forme $U_s h$ ($h \in \mathfrak{H}$, $-\infty < s < \infty$). Envisageons à cet effet la fonction $r(x) = \left(\frac{x-i}{x+i}\right)^m$ avec m entier fixé; elle est continue et de module 1 sur l'axe $-\infty < x < \infty$. Il existe alors une suite de polynomes trigonométriques

$$p_n(x) = \sum_{k=1}^{r_n} c_{n,k}\, e^{is_{n,k}x} \qquad (n = 1, 2, \ldots)$$

avec des valeurs réelles $s_{n,k}$ non nécessairement commensurables aux exposants, tels que

$$|p_n(x)| \leqq 2, \quad p_n(x) \to r(x) \quad (n \to \infty).^{11})$$

En faisant la substitution

$$x = \frac{1}{i}\frac{e^{i\Theta}+1}{e^{i\Theta}-1}, \qquad \frac{x-i}{x+i} = e^{i\Theta}$$

---

9) Cette voie d'arriver au théorème de Stone est très voisine de celle suivie par J. von Neumann [3].

10) Cas particulier d'un théorème de Sz.-Nagy et Hille, cf. [9] p. 73 ou [2] p. 375.

11) On peut choisir pour $p_n(x)$ p. ex. un polynome trigonométrique de période $4n$, s'approchant dans l'intervalle $-n \leqq x \leqq 3n$ à $1/n$ près de la fonction $r_n(x)$ qui coïncide avec $r(x)$ pour $-n \leqq x \leqq n$ et est égale à $r(2n-x)$ pour $n \leqq x \leqq 3n$.

on obtient la suite

$$q_n(e^{i\Theta}) = \sum_{k=1}^{r_n} c_{n,k}\, u_{s_{n,k}}(e^{i\Theta}),$$

$u_s(\lambda)$ étant la fonction définie par (11). Comme la suite $\{q_n(e^{i\Theta})\}$ est bornée et tend vers $e^{im\Theta}$ pour $0 < \Theta < 2\pi$, et comme U n'a pas la valeur propre 1, il découle du théorème 2 (ii) et de (11)[12]) que

$$q_n(U) = \sum_{k=1}^{r_n} c_{n,k}\, u_{s_{n,k}}(U) = \sum_{k=1}^{r_n} c_{n,k}\, U_{s_{n,k}} \to U^m \quad (n \to \infty).$$

L'espace $\mathfrak{R}$, qui est sous-tendu par les éléments de la forme $U^m h$ ($h \in \mathfrak{H}$, m entier), est donc sous-tendu aussi par les éléments $U_s h$ ($h \in \mathfrak{H}$, $-\infty < s < \infty$). De cette façon on vient de démontrer que pour tout semi-groupe continu $\{T_s\}_{s \geqq 0}$ de contractions de l'espace $\mathfrak{H}$ il existe un groupe continu $\{U_s\}_{-\infty < s < \infty}$ de transformations unitaires d'un espace $\mathfrak{K} \supseteq \mathfrak{H}$, tel que la relation (16) soit vérifiée et $\mathfrak{K}$ soit sous-tendu par les éléments de la forme $U_s h$ ($h \in \mathfrak{H}$, $-\infty < s < \infty$). Il est facile à montrer que ces propriétés de $\{U_s\}$ le déterminent d'une manière univoque[13]); nous l'appellerons *la dilatation unitaire du semi-groupe* $\{T_s\}$.

On vient de retrouver de cette manière le théorème IV de [13] (voir aussi [10] et [1]) comme une conséquence du théorème III, sur la dilatation unitaire d'une contraction[14]).

De plus on a démontré une relation entre les dilatations unitaires du semi-groupe $\{T_s\}$ et de sa cogénératrice T:

Théorème 5. *La dilatation unitaire $\{U_s\}$ d'un semi-groupe continu de contractions $\{T_s\}$ a sa cogénératrice égale à la dilatation unitaire de la cogénératrice de $\{T_s\}$.*

Corollaire 5.1. *Pour que le semi-groupe continu de contractions $\{T_s\}$ soit constitué de transformations isométriques, il faut et il suffit que sa cogénératrice T soit isométrique.*

Démonstration. Soient $\{U_s\}$, U les dilatations unitaires de $\{T_s\}$ et T, selon les cas. D'après le théorème 5, U est la cogénératrice de U_s, donc on a, en vertu du théorème 3, $T_s = u_s(T)$, $U_s = u_s(U)$. Or si T est isométrique on a $T \subseteq U$ et ceci entraîne par le corollaire 2.1 $u_s(T) \subseteq u_s(U)$, donc

---

[12]) Appliqué à U au lieu de T.

[13]) A condition qu'on ne distingue pas entre les différentes réalisations du prolongement $\mathfrak{K}$ de $\mathfrak{H}$.

[14]) A vrai dire, on suppose là au lieu de la convergence forte $T_s \to I$ ($s \to 0$) seulement la convergence faible $T_s \to I$. Or l'équivalence de ces conditions, qui est une conséquence du théorème IV cité, résulte aussi directement de certains théorèmes généraux de Dunford, cf. [2] p. 183—189.

$T_s \subseteq U_s$: T_s est isométrique. Inversement, si T_s est isométrique pour tout $s \geqq 0$, on a $T_s \subseteq U_s$ et

$$[T_s - (1-s)I][T_s - (1+s)I]^{-1} \subseteq [U_s - (1-s)I][U_s - (1+s)I]^{-1} \quad (s > 0),$$

d'où il résulte par (12) que $T \subseteq U$: T est isométrique.

Corollaire 5.2. *Si, pour un semi-groupe continu $\{T_s\}$ de contractions, la dilatation unitaire U de la cogénératrice T de $\{T_s\}$ est unitairement équivalente à la somme orthogonale de $\mathfrak{d}$ répliques ($\mathfrak{d}$ un nombre cardinal quelconque) de la transformation unitaire $Vf(\varphi) = e^{i\varphi} f(\varphi)$ de l'espace $L^2(0, 2\pi)$, la dilatation unitaire $\{U_s\}$ de $\{T_s\}$ est unitairement équivalente à la somme orthogonale de $\mathfrak{d}$ répliques du groupe unitaire $\{V_s\}$ de l'espace $L^2(-\infty, \infty)$, défini par $V_s g(x) = e^{isx} g(x)$.*

Démonstration. En vertu du théorème 5, la cogénératrice de $\{U_s\}$ est égale à U, donc on a $U_s = u_s(U)$ et par conséquent $\{U_s\}$ est unitairement équivalent à la somme orthogonale de $\mathfrak{d}$ répliques du groupe $\{W_s\}$ de l'espace $L^2(0, 2\pi)$, défini par $W_s f(\varphi) = u_s(e^{i\varphi}) f(\varphi)$. Or

$$f(\varphi) \to g(x) = \left(\frac{2}{1+x^2}\right)^{\frac{1}{2}} f(-2 \operatorname{arc\,cotg} x)$$

est une application linéaire isométrique de l'espace $L^2(0 \leqq \varphi \leqq 2\pi)$ sur l'espace $L^2(-\infty < x < \infty)$, pour laquelle

$$u_s(e^{i\varphi}) f(\varphi) \to e^{isx} g(x),$$

donc $\{W_s\}$ est unitairement équivalent au groupe $\{V_s\}$ indiqué dans le corollaire.

Remarque. En vertu d'un théorème de SCHREIBER [8] l'hypothèse du corollaire 5.2 est vérifiée pour toute contraction au sens strict T (c'est-à-dire pour laquelle $\|T\| < 1$), notamment avec $\mathfrak{d} = \dim \mathfrak{H}$.[15]) De cette façon le théorème 3 de l'article [12], sur les semi-groupes de contractions dont la cogénératrice est une contraction au sens strict, apparaît comme une conséquence du théorème de SCHREIBER.

III.

6. D'après J. VON NEUMANN [4], un ensemble fermé S de points du plan complexe s'appelle un *ensemble spectral* de la transformation linéaire bornée T de l'espace de Hilbert $\mathfrak{H}$ si, pour toute fonction rationnelle $r(\lambda)$ bornée

[15]) Dans [8] on suppose que $\dim \mathfrak{H} \leqq \aleph_0$; une démonstration valable pour $\mathfrak{H}$ de dimension quelconque a été donnée dans l'article [12].

sur S, la transformation $r(T)$ existe[16]) et on a

$$\|r(T)\| \leqq \sup_{\lambda \in S} |r(\lambda)|. \tag{17}$$

Il s'ensuit immédiatement de cette définition que le spectre de T, $\sigma(T)$, doit être contenu dans S. Pour T normale, $\sigma(T)$ est lui-même un ensemble spectral de T, mais pour T non-normale cela n'est pas toujours le cas. Tout ensemble fermé qui contient un ensemble spectral de T est évidemment lui-même un ensemble spectral de T. Le disque $|\lambda| \leqq \|T\|$ est toujours un ensemble spectral de T et en particulier le disque unité S_0 est ensemble spectral de toute contraction.[17])

S étant un ensemble spectral de T, VON NEUMANN appelle une fonction $u(\lambda)$ *S-analytique* si elle est limite sur S d'une suite uniformément convergente de fonctions rationnelles $r_n(\lambda)$ ayant leurs pôles à l'extérieur de S (c'est-à-dire dans la partie complémentaire CS du plan complexe). De (17) il s'ensuit que les transformations $r_n(T)$ tendent alors en norme vers une limite, indépendante du choix particulier de la suite $\{r_n(\lambda)\}$, et qu'on peut alors désigner par $u(T)$; c'est une transformation linéaire bornée telle que

$$\|u(T)\| \leqq \sup_{\lambda \in S} |u(\lambda)|. \tag{17'}$$

Les fonctions S-analytiques forment évidemment une algèbre, et l'application $u(\lambda) \to u(T)$ est linéaire et multiplicative. De plus, si l'image de S par la fonction S-analytique $\lambda' = u(\lambda)$ est un ensemble fermé S', (i) S' est un ensemble spectral de $T' = u(T)$, (ii) pour toute fonction S'-analytique $v(\lambda')$ la fonction composée $v \circ u(\lambda) = v(u(\lambda))$ est S-analytique et on a $v \circ u(T) = v(T')$.

Tous ces faits simples se trouvent établis dans le Mémoire cité de VON NEUMANN. Voici quelques remarques additionnelles.

Tout d'abord remarquons que si S est un ensemble spectral de T,

(18) $Th = \mu h$ (pour un $\mu \in S$ et un $h \in \mathfrak{H}$) *entraîne* $u(T)h = u(\mu)h$

pour toute fonction S-analytique $u(\lambda)$. En effet, cette implication est immédiate pour $r(\lambda)$ rationnelle ayant ses pôles à l'extérieur de S; pour $u(\lambda)$ S-analytique de type général elle s'ensuit alors par un passage à la limite $r_n(\lambda) \to u(\lambda)$, uniforme sur S.

---

[16]) Pour $r(\lambda) = c \prod_i (\lambda - a_i) \prod_j (\lambda - b_j)^{-1}$ $(a_i \neq b_j)$ on définit $r(T)$ directement par $c(T - a_i I)(T - b_j I)^{-1}$ à condition qu'aucun des pôles b_j n'appartient au spectre de T.

[17]) Par raison d'homogénéité il suffit d'envisager le cas où $\|T\| \leqq 1$. Or, dans ce cas, ce résultat de VON NEUMANN est un corollaire du théorème sur l'existence de la dilatation unitaire U de T; en effet, on a $r(T) = \mathrm{pr}\, r(U)$, $\|r(T)\| \leqq \|r(U)\| \leqq \sup_{|\lambda|=1} r(\lambda)$ (voir (6)).

Pour commodité de langage donnons la définition suivante:

Définition 3. *Soit $\bar{\mathcal{O}}(S)$ la classe des fonctions qui sont continues dans S et holomorphes dans tout point intérieur de S.*

Il est manifeste que toute fonction S-analytique appartient à $\bar{\mathcal{O}}(S)$. Dans le cas particulier où S est un ensemble borné dont la frontière ∂S est une courbe simple fermée (bref: si S est un *ensemble jordanien borné*), un théorème de WALSH affirme (voir [14] p. 36) que toute fonction qui est continue sur S et holomorphe dans l'intérieur de S est limite uniforme sur S de polynômes. Donc, *pour les ensembles jordaniens bornés, la classe des fonctions S-analytiques coïncide avec la classe $\bar{\mathcal{O}}(S)$.*

Soient S et S' deux ensembles jordaniens bornés. Soit $\lambda \to \lambda' = s(\lambda)$ une *application conforme* de S sur S'[18]), et soit $\lambda' \to \lambda = \bar{s}^{-1}(\lambda')$ l'application conforme inverse. On a évidemment $s(\lambda) \in \bar{\mathcal{O}}(S)$ et $\bar{s}^{-1}(\lambda') \in \bar{\mathcal{O}}(S')$. Si S est un ensemble spectral de la transformation T, S' est un ensemble spectral de la transformation $T' = s(T)$, et on a inversement $T = \bar{s}^{-1}(T')$. En vertu de (18) les équations

$$Th = \mu h, \quad T'h = \mu' h$$

(où μ, μ' sont deux points de S et S' correspondants par l'application conforme envisagée) s'entraînent mutuellement. Il s'ensuit en particulier que le spectre ponctuel de T' est l'image du spectre ponctuel de T.

Dans ce qui suit on choisira pour S' le disque unité fermé S_0 et on désignera $s(T)$ par T_0, c'est une *contraction*. Soit U_0 la dilatation unitaire de T_0, opérant dans l'espace $\mathfrak{H} \supseteq \mathfrak{H}$, et soit $N = \bar{s}^{-1}(U_0)$.[19]) Comme fonction de la transformation unitaire U_0, N est une transformation *normale*; son spectre est l'image par l'application $\lambda_0 \to \lambda = \bar{s}^{-1}(\lambda_0)$ du spectre de U_0 et par conséquent est situé sur ∂S (la frontière de S). Comme on a $u(T_0) = \mathrm{pr}\, u(U_0)$ pour toute fonction $u(\lambda_0) \in \bar{\mathcal{O}}(S_0)$,[19]) il s'ensuit que, en particulier,

$$T^n = [\bar{s}^{-1}(T_0)]^n = \bar{s}^{-1n}(T_0) = \mathrm{pr}\,[\bar{s}^{-1n}(U_0)] = \mathrm{pr}\,[\bar{s}^{-1}(U_0)]^n = \mathrm{pr}\, N^n$$

($n = 0, 1, 2, \ldots$). Montrons que les éléments de la forme $N(n)h$[20]) ($h \in \mathfrak{H}$,

---

[18]) Nous entendrons par là une application conforme (proprement dite) de l'intérieur de S sur l'intérieur de S', prolongée (en vertu du théorème de CARATHÉODORY) à une application topologique de S sur S'.

[19]) La classe $\bar{\mathcal{O}}(S_0)$ est évidemment contenue dans toute classe $\mathcal{O}_R(S_0)$ où R est une contraction (voir § 2), et pour $u(\lambda_0) \in \bar{\mathcal{O}}(S_0)$ la définition actuelle de $u(R)$ coïncide avec celle donnée au § 2. Cela est immédiat pour les polynômes de λ_0, et de là on passe au cas d'une fonction $u(\lambda_0) \in \bar{\mathcal{O}}(S_0)$ de type général par l'intermédiaire d'une suite de polynômes convergeant vers $u(\lambda_0)$ uniformément sur S_0.

[20]) $N(n) = N^n$ ou $= N^{*n}$ selon que $n \geqq 0$ ou $n < 0$.

$n = 0, \pm 1, \pm 2, \ldots$) sous-tendent l'espace $\mathfrak{N}$. Envisageons à cet effet la fonction $s^m(\lambda)$ sur ∂S, m étant un entier fixé quelconque. Cette fonction est continue sur ∂S et par conséquent elle peut être approchée uniformément sur ∂S par la somme d'un polynôme de λ et d'un polynôme de $\bar{\lambda}$ (cf. [14] p. 39). La transformation $U_0''' = s'''(N)$ peut donc être approchée en norme par la somme d'un polynôme de N et d'un polynôme de N^* (nous faisons ici usage de la formule (7) pour les fonctions de type général d'une transformation normale où, dans ce cas, il suffit d'intégrer sur ∂S). Pour tout $h \in \mathfrak{H}$, $U_0''' h$ est donc limite de combinaisons linéaires des éléments $N(n)h$. Or les éléments de la forme $U_0''' h$ sous-tendent l'espace $\mathfrak{N}$, donc les éléments de la forme $N(n)h$ le sous-tendent aussi.

Supposons que N' soit une autre transformation normale, opérant dans un espace $\mathfrak{N}' \supseteq \mathfrak{H}$, telle que $\sigma(N') \subseteq \partial S$, $T'' = \mathrm{pr}\, N'^n$ $(n = 0, 1, 2, \ldots)$ et que les éléments de la forme $N'(n)h$ $(h \in \mathfrak{H}; n = 0, \pm 1, \pm 2, \ldots)$ sous-tendent l'espace $\mathfrak{N}'$. Soit $U_0' = s(N')$; puisque $|s(\lambda)| = 1$ sur ∂S donc sur $\sigma(N')$, U_0' est unitaire. Le même raisonnement qui nous a conduits des propriétés de U_0 à celles de N, suivi dans la direction opposée $N' \to U_0'$, fournit que $T_0'' = \mathrm{pr}\, U_0'^n$ $(n = 0, 1, 2, \ldots)$ et que l'espace $\mathfrak{N}'$ est sous-tendu par les éléments de la forme $U_0'(n)h = U_0'^n h$ $(h \in \mathfrak{H}; n = 0, \pm 1, \pm 2, \ldots)$. Or la dilatation unitaire d'une contraction est déterminée de manière univoque, c'est-à-dire à un isomorphisme près, donc il existe une application linéaire et isométrique τ de $\mathfrak{N}$ sur $\mathfrak{N}'$, laissant invariants les éléments de $\mathfrak{H}$, et telle que $U_0' = \tau U_0 \tau^{-1}$. Cela entraîne que $p(U_0') = \tau p(U_0)\tau^{-1}$ pour tout polynôme $p(\lambda)$ et alors $u(U_0') = \tau\, u(U_0)\tau^{-1}$ pour toute fonction $u(\lambda_0) \in \bar{\mathfrak{S}}(S_0)$, en particulier on a $\bar{s}^{-1}(U_0') = \tau \bar{s}^{-1}(U_0)\tau^{-1}$, donc $N' = \tau N \tau^{-1}$. En d'autres termes, si l'on identifie les éléments de $\mathfrak{N}$ et $\mathfrak{N}'$ qui se correspondent par τ, N' coïncidera avec N.

En résumant, nous avons démontré le

Théorème 6. *S étant un ensemble spectral jordanien borné de la transformation linéaire bornée T de l'espace $\mathfrak{H}$, il existe, dans un espace $\mathfrak{N} \supseteq \mathfrak{H}$, une transformation normale N telle que le spectre de N est situé sur la frontière de S, et que*

$$T'' = \mathrm{pr}\, N'' \qquad (n = 0, 1, 2, \ldots);$$

en plus, $\mathfrak{N}$ est sous-tendu par les éléments de la forme $N''h$ et $N^{*n}h$ $(h \in \mathfrak{H}; n = 0, 1, 2, \ldots)$. Ces conditions déterminent N de manière univoque[21]*. Si $\lambda_0 = s(\lambda)$ est une application conforme de S sur le disque unité fermé S_0, $s(N)$ est la dilatation unitaire de la contraction $s(T)$.*

[21]) A condition qu'on ne distingue pas entre les différentes réalisations du prolongement $\mathfrak{N}$ de $\mathfrak{H}$.

Appelons cette transformation *N la dilatation normale de T par rapport à l'ensemble spectral S.*

7. Voici quelques relations spectrales entre T et N qui dérivent de manière plus ou moins immédiate des relations entre une contraction et sa dilatation unitaire.

Théorème 7. (i) *On a* $T \subseteqq N$ *si* $s(T)$ *est isométrique, et dans ce cas seulement.* (ii) *Si* $T \neq N$, *c'est-à-dire si T n'est pas elle-même normale ayant son spectre situé sur la frontière de S, le spectre de N recouvre toute la frontière de S.* (iii) *Toute valeur propre de T sur la frontière de S est en même temps une valeur propre de N et inversement, et les vecteurs propres correspondants sont les mêmes pour T et N.*[22]) (iv) *Si S contient dans son intérieur un autre ensemble spectral de T, la dilatation normale N de T par rapport à S est unitairement équivalente à la somme orthogonale de* $\mathfrak{d}$ *répliques* ($\mathfrak{d} = \dim \mathfrak{H}$) *de la transformation normale* N_S *de l'espace* $L^2(0, 2\pi)$, *définie par* $N_S f(\varphi) = \bar{s}^{-1}(e^{i\varphi}) f(\varphi)$ *où* $e^{i\varphi} \to \bar{s}^{-1}(e^{i\varphi})$ *est l'application topologique du cercle unité sur la frontière de S, induite par l'application conforme* $\lambda_0 \to \bar{s}^{-1}(\lambda_0)$ *du disque unité* S_0 *sur S.*[23])

Démonstration. *Ad* (i): Si $T_0 = s(T)$ est isométrique, on a $T_0 \subseteqq U_0$, donc, en vertu du corollaire 2.1, $T = \bar{s}^{-1}(T_0) \subseteqq \bar{s}^{-1}(U_0) = N$. Inversement, si $T \subseteqq N$, on a $p(T) \subseteqq p(N)$ pour tout polynôme $p(\lambda)$, d'où il s'ensuit $u(T) \subseteqq u(N)$ pour toute fonction $u(\lambda) \in \mathfrak{C}(S)$, en particulier on a $s(T) \subseteqq s(N)$, donc $T_0 \subseteqq U_0$: T_0 est isométrique. *Ad* (ii): Le spectre de $U_0 = s(N)$ étant l'image du spectre de N par l'application $\lambda \to s(\lambda)$, si $\sigma(N)$ ne recouvre pas ∂S, $\sigma(U_0)$ ne recouvre pas le cercle unité; or en vertu du corollaire 2.2 cela entraîne que $T_0 = U_0$, et alors $T = \bar{s}^{-1}(T_0) = \bar{s}^{-1}(U_0) = N$. *Ad* (iii): Puisqu'on a les relations $T_0 = s(T)$ et $T = \bar{s}^{-1}(T_0)$, il s'ensuit de (18) que les équations

$$Th = \mu h, \quad T_0 h = \mu_0 h \qquad (\text{où } \mu_0 = s(\mu))$$

s'entraînent mutuellement; par la même raison, les équations

$$Nh = \mu h, \quad U_0 h = \mu_0 h$$

s'entraînent aussi mutuellement. Or, si μ est sur ∂S, μ_0 est sur le cercle unité, et les équations

$$T_0 h = \mu_0 h, \quad U_0 h = \mu_0 h$$

---

[22]) Par conséquent deux vecteurs propres de T correspondant à deux valeurs propres différentes, situées sur ∂S, sont orthogonaux.

[23]) On peut choisir cette application conforme d'ailleurs arbitrairement.

s'entraînent mutuellement en vertu du théorème 1. Par conséquent, pour μ situé sur ∂S, les équations

$$Th = \mu h, \quad Nh = \mu h$$

s'entraînent mutuellement. *Ad* (iv): Si T a un ensemble spectral S_1 situé dans *l'intérieur* de S, $T_0 = s(T)$ aura l'ensemble spectral $s(S_1)$ situé dans l'intérieur du disque unité S_0, ce qui entraîne que $\|T_0\| < 1$. Or par le théorème de SCHREIBER (voir [8], [12]) la dilatation unitaire U_0 de T_0 est alors unitairement équivalente à la somme orthogonale de $\mathfrak{d}$ répliques de la transformation unitaire $Vf(\varphi) = e^{i\varphi} f(\varphi)$ de l'espace $L^2(0, 2\pi)$. Puisqu'on a $N = \bar{s}^{-1}(U_0)$, l'assertion en découle immédiatement.

8. Soit S un ensemble spectral jordanien borné de la transformation T. Nous allons indiquer comment le calcul fonctionnel pour T peut être étendu au delà de la classe $\bar{\mathcal{C}}(S)$, et cela en faisant usage du calcul fonctionnel pour les contractions, envisagé au paragraphe 2.

Soient, comme plus haut, $\lambda_0 = s(\lambda)$ une application conforme de S sur le disque unité S_0 et $\lambda = \bar{s}^{-1}(\lambda_0)$ son inverse; soit $T_0 = s(T)$, donc $T = \bar{s}^{-1}(T_0)$. Cela étant, convenons de la définition suivante:

Définition 4. *Nous dirons que la fonction $u(\lambda)$, définie dans l'intérieur de S, appartient à la classe $\mathcal{C}_T(S)$, lorsque la fonction $u \circ \bar{s}^{-1}(\lambda_0)$, définie dans l'intérieur de S_0, appartient à la classe $\mathcal{C}_{T_0}(S_0)$ correspondant à la contraction T_0 d'après la définition 2 donnée au paragraphe 2, et dans ce cas nous posons par définition*

$$u(T) = u \circ \bar{s}^{-1}(T_0).$$

Il est manifeste que cette classe comprend en particulier toutes les fonctions $u(\lambda)$ qui sont holomorphes dans l'intérieur de S et continues dans S sauf au plus en un ensemble dénombrable de points à la frontière, dont aucun n'est une valeur propre de T (en ces points exceptionnels $u(\lambda)$ peut même ne pas être définie). $\mathcal{C}_T(S)$ comprend en particulier la classe $\bar{\mathcal{C}}(S)$, et comme, en vertu de la règle de composition des fonctions S-analytiques, $u \in \bar{\mathcal{C}}(S)$ entraîne $u \circ \bar{s}^{-1} \in \bar{\mathcal{C}}(S_0)$ et $u \circ \bar{s}^{-1}(T_0) = u[\bar{s}^{-1}(T_0)] = u(T)$, on voit que la nouvelle définition de $u(T)$ est consistente avec celle donnée au paragraphe 6. [24])

Théorème 8.1. *La classe $\mathcal{C}_T(S)$ et la définition de $u(T)$ sur cette classe ne dépendent pas du choix particulier de l'application conforme $\lambda_0 = s(\lambda)$ de S sur S_0.*

---

[24]) De la "propriété 4.3" dans [1] il résulte par la même voie que la classe γ définie $\bar{\mathcal{C}}_e[S; T]$ est contenue dans la classe $\mathcal{C}_T(S)$ du présent travail et que les deux définitions des fonctions de T sont consistentes.

Démonstration. Si $\lambda_0 = s'(\lambda)$ est une autre application conforme de S sur S_0, $\lambda_0 = s' \circ \bar{s}^{-1}(\lambda_0) \equiv l(\lambda_0)$ sera une application conforme de S_0 sur S_0, donc une homographie. On aura $T_0' = s'(T) = s'[\bar{s}^{-1}(T_0)] = s' \circ \bar{s}^{-1}(T_0) = l(T_0)$, donc, en vertu du théorème 2 (iv), $v \in \mathcal{O}_{T_0'}(S_0)$ entraîne $v \circ l \in \mathcal{O}_{T_0}(S_0)$ et $v(T_0') = v \circ l(T_0)$. Par conséquent si $u(\lambda)$ est une fonction définie dans l'intérieur de S, telle que $u \circ \bar{s}^{-1} \in \mathcal{O}_{T_0'}(S_0)$, on aura $u \circ \bar{s}^{-1} = u \circ (\bar{s}'^{-1} \circ s') \circ \bar{s}^{-1} = (u \circ \bar{s}'^{-1}) \circ l \in \mathcal{O}_{T_0}(S_0)$ et $u \circ \bar{s}^{-1}(T_0') = u \circ \bar{s}^{-1}(T_0)$. Les rôles de s et s' étant symétriques, cela démontre l'indépendence de la définition du choix particulier de l'application conforme.

Les propriétés de *linéarité*, de *multiplicativité* et de *convergence* établies au théorème 2 (i) – (ii) se transportent à la classe $\mathcal{O}_T(S)$ de manière évidente. Formulons les propriétés suivantes pour les fonctions composées:

Théorème 8.2. *Soit S un ensemble spectral jordanien borné de la transformation T et soit $u \in \mathcal{O}_T(S)$, $T' = u(T)$.*

(i) *Le spectre de T' est contenu dans l'adhérence $\bar{Z}$ de l'ensemble Z des valeurs prises par $u(\lambda)$ dans l'intérieur de S. Pour toute fonction $w(z)$, holomorphe dans un domaine contenant l'ensemble (borné, fermé et connexe) $\bar{Z}$ dans son intérieur, on a*

$$w \circ u \in \mathcal{O}_T(S) \quad et \quad w \circ u(T) = w^{\mathrm{R}}(T'),$$

la lettre R *indiquant qu'il s'agit là de la définition au sens du calcul fonctionnel de Riesz—Dunford* (cf. [7] n° 151).

(ii) *Si, en particulier, $\lambda' = u(\lambda)$ est une application conforme de S sur un ensemble jordanien borné S', on a pour toute fonction $v \in \mathcal{O}_{T'}(S')$:*

$$v \circ u \in \mathcal{O}_T(S) \quad et \quad v \circ u(T) = v(T').$$

Démonstration. L'assertion (i) est une conséquence immédiate du théorème 2 (v); en effet on a en vertu de ce théorème

$$w \circ u(T) = w \circ u \circ \bar{s}^{-1}(T_0) = w^{\mathrm{R}}(u \circ \bar{s}^{-1}(T_0)) = w^{\mathrm{R}}(u(T)),$$

où $\lambda_0 = s(\lambda)$ est une application conforme de S sur S_0, et $T_0 = s(T)$.

Dans le cas (ii) posons $s' = s \circ \bar{u}^{-1}$; $\lambda_0 = s'(\lambda')$, est alors une application conforme de S' sur S_0. Soit $T_0' = s'(T')$. En vertu de la règle de composition des fonctions S-analytiques on a

$$T_0' = s \circ \bar{u}^{-1}(T') = s(\bar{u}^{-1}(T')) = s(T) = T_0.$$

L'hypothèse $v \in \mathcal{O}_{T'}(S')$ est équivalente à ce que $v \circ \bar{s}'^{-1} \in \mathcal{O}_{T_0'}(S_0)$, et on a par la définition 4:

$$v(T') = v \circ \bar{s}'^{-1}(T_0') = v \circ (u \circ \bar{s}^{-1})(T_0') = v \circ u \circ \bar{s}^{-1}(T_0') = v \circ u \circ \bar{s}^{-1}(T_0) = v \circ u(T),$$

ce qui achève la démonstration.

Observons encore, pour terminer, le fait suivant:

Théorème 8.3. *Si N est la dilatation normale de T par rapport à l'ensemble spectral jordanien borné S, les classes $\mathcal{C}_T(S)$ et $\mathcal{C}_N(S)$ coïncident, et pour $u \in \mathcal{C}_T(S)$ on a*

$$u(T) = \operatorname{pr} u(N). \tag{19}$$

Démonstration. Si $\lambda_0 = s(\lambda)$ est une application conforme de S sur S_0, $U_0 = s(N)$ est la dilatation unitaire de $T_0 = s(T)$ (voir théorème 6) et par conséquent les classes $\mathcal{C}_{T_0}(S_0)$ et $\mathcal{C}_{U_0}(S_0)$ coïncident, et pour $v \in \mathcal{C}_{T_0}(S_0)$ on a par définition $v(T_0) = \operatorname{pr} v(U_0)$. En choisissant en particulier $v = u \circ \tilde{s}^{-1}$, il résulte l'équation (19).

Ouvrages cités.

[1] C. Foias, La mesure harmonique-spectrale et la théorie spectrale des opérateurs généraux de l'espace de Hilbert, *Bulletin Soc. Math. de France* (à apparaître).

[2] E. Hille, *Functional analysis and semi-groups* (New York, 1948).

[3] J. von Neumann, Über einen Satz von Herrn M. H. Stone, *Annals of Math.*, **33** (1932), 567—573.

[4] ——— Eine Spektraltheorie für allgemeine Operatoren eines unitären Raumes, *Math. Nachrichten*, **4** (1951), 258—281.

[5] A. Plessner, Über Funktionen eines maximalen Operators, *Comptes Rendus (Doklady) Acad. Sci. URSS*, **23** (1939), 327—330.

[6] ——— Über halbunitäre Operatoren, *ibidem*, **25** (1939), 710—712.

[7] F. Riesz—B. Sz.-Nagy, *Leçons d'analyse fonctionnelle*, 3. édition (Budapest—Paris, 1955).

[8] M. Schreiber, Unitary dilations of operators, *Duke Math. Journal*, **23** (1956), 579—594.

[9] B. Sz.-Nagy, *Spektraldarstellung linearer Transformationen des Hilbertschen Raumes*, Ergebnisse d. Math. u. ihrer Grenzgebiete, V/5 (Berlin, 1942).

[10] ——— Sur les contractions de l'espace de Hilbert, *Acta Sci. Math.*, **15** (1953), 87—92.

[11] ——— Transformations de l'espace de Hilbert, fonctions de type positif sur un groupe, *ibidem*, **15** (1954), 104—114.

[12] ——— Sur les contractions de l'espace de Hilbert. II, *ibidem*, **18** (1957), 1—15.

[13] ——— *Prolongements des transformations de l'espace de Hilbert qui sortent de cet espace.* Appendice au livre "Leçons d'analyse fonctionnelle" par F. Riesz et B. Sz.-Nagy (Budapest, 1955).

[14] J. L. Walsh, *Interpolation and approximation by rational functions in the complex domain* (New York, 1935).

(Reçu le 1 novembre 1957.)

On a mean-value theorem of Schwarz—Stieltjes.*)

By PAUL SZÁSZ in Budapest.

Let $f(x)$ be a single-valued function of the real variable x, which has derivatives of the first n orders throughout the open interval (a, b). Let the real numbers $a_0, \ldots, a_k$ and the positive integers $m_0, \ldots, m_k$ be chosen such that

$$a < a_0 < a_1 < \cdots < a_k < b$$

and

$$m_0 + m_1 + \cdots + m_k = n + 1. \tag{1}$$

If, following N. E. NÖRLUND[1]), we denote by

$$[\overbrace{a_0, \ldots, a_0}^{m_0 \text{ times}}, \overbrace{a_1, \ldots, a_1}^{m_1 \text{ times}}, \ldots, \overbrace{a_k, \ldots, a_k}^{m_k \text{ times}}; f(x)]$$

the coefficient of x^n in the polynomial $H(x)$ of order $\leqq n$ satisfying the interpolatory conditions

$$H(a_i) = f(a_i),\ H'(a_i) = f'(a_i), \ldots, H^{(m_i-1)}(a_i) = f^{(m_i-1)}(a_i) \quad (i = 0, 1, \ldots, k) \tag{2}$$

of CH. HERMITE[2]), then the mean-value theorem

$$[\overbrace{a_0, \ldots, a_0}^{m_0 \text{ times}}, \overbrace{a_1, \ldots, a_1}^{m_1 \text{ times}}, \ldots, \overbrace{a_k, \ldots, a_k}^{m_k \text{ times}}; f(x)] = \frac{f^{(n)}(\xi)}{n!} \tag{3}$$

of SCHWARZ—STIELTJES[3]) is valid, where $a_0 < \xi < a_k$.

---

*) Abbreviated version of a previous paper of the author in Hungarian: A differenciálszámítás középértéktételével kapcsolatos kérdésekről, *Mathematikai és Physikai Lapok*, **33** (1926), 150—180.

[1]) N. E. NÖRLUND, *Leçons sur les séries d'interpolation* (Paris, 1926), p. 7—8.

[2]) CH. HERMITE, Sur la formule d'interpolation de Lagrange, *Journal für die reine und angewandte Math.*, **84** (1878), 70—79, in particular p. 70, or *Oeuvres de Charles Hermite*, III (Paris, 1912), p. 432—443, in particular p. 432.

[3]) H. A. SCHWARZ, Démonstration élémentaire d'une propriété fondamentale des fonctions interpolaires, *Gesammelte mathematische Abhandlungen II* (Berlin, 1890), p. 307—308, in particular p. 308; further T. J. STIELTJES, A propos de la formule d'interpolation de Lagrange, *Oeuvres complètes de Thomas Jan Stieltjes* I (Groningen, 1914), p. 47—60, in particular p. 56. H. A. SCHWARZ stated the theorem only in the case $k = n$ and supposed the continuity of $f^{(n)}(x)$.

In the case

$$k=n,\ a_0=\alpha,\ a_1=\alpha+h,\ \ldots,\ a_n=\alpha+nh$$

(3) can be written in the form

$$(M_n) \qquad \Delta^n f(\alpha)=h^n f(\alpha+\tau nh) \qquad (0<\tau<1)$$

while for

$$k=1,\ a_0=\alpha,\ a_1=\alpha+h,\ m_0=n,\ m_1=1$$

from (3) it follows TAYLOR's mean-value theorem with LAGRANGE's form of the remainder:

$$(T_n) \quad f(\alpha+h)=f(\alpha)+\frac{h}{1!}f'(\alpha)+\cdots+\frac{h^{n-1}}{(n-1)!}f^{(n-1)}(\alpha)+\frac{h^n}{n!}f^{(n)}(\alpha+\vartheta h)$$
$$(0<\vartheta<1)$$

It has been proved by R. ROTHE[4]), that in (M_n)

$$\tau\to\frac{1}{2} \quad \text{for} \quad h\to 0 \tag{4}$$

and in (T_n)

$$\vartheta\to\frac{1}{n+1} \quad \text{for} \quad h\to 0, \tag{5}$$

assumed in both cases that $f^{(n+1)}(x)$ exists in the neighbourhood of the point α, and is continuous and $\neq 0$ in α.[5]) I have shown[6]), that it is sufficient to suppose the existence of $f^{(n+1)}(\alpha)\neq 0$.

In the present paper I shall prove first the following theorem, which contains the above theorems (4) and (5):

Theorem I. *Suppose the points a_0, a_k tend to the point α of the open interval (a, b) with the restriction*

$$\left|\frac{a_0-\alpha}{a_k-a_0}\right|\leqq L., \qquad \left|\frac{a_k-\alpha}{a_k-a_0}\right|\leqq L. \tag{6}$$

Then for the mean-value ξ in (3) we have

$$\frac{1}{a_k-a_0}\left(\xi-\frac{m_0a_0+m_1a_1+\cdots+m_ka_k}{m_0+m_1+\cdots+m_k}\right)\to 0, \tag{7}$$

assumed that $f^{(n+1)}\alpha$ exists and is $\neq 0$.

---

[4]) R. ROTHE, Zum Mittelwertsatze der Differentialrechnung, *Math. Zeitschrift*, **9** (1921), 300—325, in particular p. 314, further p. 309—310.

[5]) The latter theorem has been proved by M. BEKE, *Differenciál- és integrálszámitás* I. (in Hungarian), (Budapest, 1910), p. 197.

[6]) PAUL SZÁSZ, Über einen Mittelwertsatz, *Math. Zeitschrift*, **25** (1926), 116—120. Later the same was proved for TAYLOR's mean-value theorem (T_n) by CHR. Y. PAUC, see OTTO HAUPT—GEORG AUMANN, *Differential- und Integralrechnung*, 2. Aufl. unter Mitwirkung von CHRISTIAN Y. PAUC, II. Band (Berlin, 1950), p. 42.

I need the following

Lemma. *We have*

$$(8)\quad [\overbrace{a_0,\ldots,a_0}^{m_0 \text{ times}},\ \overbrace{a_1,\ldots,a_1}^{m_1 \text{ times}},\ \ldots,\ \overbrace{a_k,\ldots,a_k}^{m_k \text{ times}};\ x^{n+1}] = m_0a_0 + m_1a_1 + \cdots + m_ka_k.$$

Proof of the lemma. In (2) choose $f(x)=x^{n+1}$. Then the roots of the algebraic equation

$$(9)\quad x^{n+1} - H(x) = 0$$

are

$$\overbrace{a_0,\ldots,a_0}^{m_0 \text{ times}},\ \overbrace{a_1,\ldots,a_1}^{m_1 \text{ times}},\ \ldots,\ \overbrace{a_k,\ldots,a_k}^{m_k \text{ times}}$$

every root being taken according to its multiplicity. The sum of these roots of the equation (9) is equal to the coefficient of x^n in $H(x)$, i. e. to the left-hand side of (8), which proves the Lemma.

Proof of theorem I. Let the mean-value theorem (3) be applied to the function

$$f(x) - \frac{f^{(n+1)}(\alpha)}{(n+1)!}\,x^{n+1}.$$

On the basis of the above Lemma it follows with regard to (3)

$$\frac{f^{(n)}(\xi)}{n!} - \frac{f^{(n+1)}(\alpha)}{(n+1)!}(m_0a_0 + m_1a_1 + \cdots + m_ka_k) = \frac{f^{(n)}(\xi')}{n!} - \frac{f^{(n+1)}(\alpha)}{n!}\,\xi'$$
$$(a_0 < \xi < a_k,\ a_0 < \xi' < a_k),$$

or written in another form

$$(10)\quad f^{(n+1)}(\alpha)\left(\xi - \frac{m_0a_0 + m_1a_1 + \cdots + m_ka_k}{n+1}\right) = f^{(n)}(\xi') - f^{(n)}(\xi) + f^{(n+1)}(\alpha)(\xi - \xi').$$

But we have by the definition of the derivative

$$f^{(n)}(x) = f^{(n)}(\alpha) + \{f^{(n+1)}(\alpha) + \varepsilon(x)\}(x-\alpha)$$

with

$$(11)\quad \lim_{x=\alpha} \varepsilon(x) = 0.$$

Therefore we obtain from (10)

$$f^{(n+1)}(\alpha)\left(\xi - \frac{m_0a_0 + m_1a_1 + \cdots + m_ka_k}{n+1}\right) = (\xi' - \alpha)\varepsilon(\xi') - (\xi - \alpha)\varepsilon(\xi),$$

hence with respect to (1)

$$\frac{1}{a_k-a_0}\left(\xi-\frac{m_0a_0+m_1a_1+\cdots+m_ka_k}{m_0+m_1+\cdots+m_k}\right)= \tag{12}$$
$$=\frac{1}{f^{(n+1)}(\alpha)}\left\{\frac{\xi'-\alpha}{a_k-a_0}\varepsilon(\xi')-\frac{\xi-\alpha}{a_k-a_0}\varepsilon(\xi)\right\}.$$

In consequence of the restriction (6) we have however

$$\left|\frac{\xi-\alpha}{a_k-a_0}\right|<L,\quad \left|\frac{\xi'-\alpha}{a_k-a_0}\right|<L.$$

Thus on the basis of (11), from (12) it follows (7), q. e. d.

Next we make another remark concerning the mean-value ξ in the formula (3). In case of a polynomial $f(x)$ of the exact order $n+1$, it follows at once that

$$\xi=\frac{m_0a_0+m_1a_1+\cdots+m_ka_k}{m_0+m_1+\cdots+m_k}.$$

This fact can be generalized in the following manner:

Theorem II. *Let $f^{(n)}(x)$ monotone throughout the interval $a_0<x<a_k$, further let the difference-quotient*

$$\varphi(u,v)=\frac{f^{(n)}(u)-f^{(n)}(v)}{u-v}$$

be bounded for $a_0<u<v<a_k$, and M, μ denote the upper and lower bound of $|\varphi(u,v)|$, respectively. Then in case $M\neq 0$ we have

$$\frac{1}{a_k-a_0}\left|\xi-\frac{m_0a_0+m_1a_1+\cdots+m_ka_k}{m_0+m_1+\cdots+m_k}\right|\leqq 1-\frac{\mu}{M}. \tag{13}$$

Equality is valid if and only if $M=\mu$.

Proof. Similarly to the proof of (10) we obtain

$$M\left(\xi-\frac{m_0a_0+m_1a_1+\cdots+m_ka_k}{n+1}\right)=f^{(n)}(\xi'')-f^{(n)}(\xi)+M(\xi-\xi'') \tag{14}$$
$$(a_0<\xi<a_k,\ a_0<\xi''<a_k).$$

In case $\xi''=\xi$ the assertion is obvious. Now let $\xi''\neq\xi$. From (14) and (1) it follows in consequence of

$$\left|\frac{\xi-\xi''}{a_k-a_0}\right|<1$$

that

$$\frac{1}{a_k-a_0}\left|\xi-\frac{m_0a_0+m_1a_1+\cdots+m_ka_k}{m_0+m_1+\cdots+m_k}\right|\leqq\frac{1}{M}\left(M-\frac{f^{(n)}(\xi)-f^{(n)}(\xi'')}{\xi-\xi''}\right). \tag{15}$$

It can be assumed that $f^{(n)}(x)$ does not decrease, ξ, M, μ being the same for $f(x)$ as for $-f(x)$. Then we have

$$\mu \leqq \frac{f^{(n)}(\xi) - f^{(n)}(\xi'')}{\xi - \xi''} \leqq M \tag{16}$$

and from (15), (16) it follows (13). In (15) equality is valid only in the case if the right-hand side vanishes. Consequently, in (13) equality holds if and only if $M = \mu$. Thus the proof of Theorem II is complete.

With the help of Theorem II it is easy to see, for ex., that in the well-known formula

$$\log(N+\nu) = \log N + \nu\{\log(N+1) - \log N\} - \frac{\nu(\nu+1)}{2}\frac{1}{\xi^2}$$
$$(N > 0,\ 0 < \nu < 1,\ N < \xi < N+1)$$

we have

$$\xi = N + \frac{\nu+1}{3} + \sigma$$

with

$$|\sigma| < \frac{3}{N} + \frac{3}{N^2} + \frac{1}{N^3}.$$

(Received December 28, 1957.)

Über eine neue Erweiterung von Ringen. I.

Von J. SZÉP in Szeged.

§ 1. Einleitung.

Wir betrachten einen Ring R mit zwei Unterringen A und B so beschaffen, daß die Beziehungen

$$(\mathfrak{A}) \qquad R^+ = A^+ + B^+, \quad A \cap B = 0$$

gelten, wobei mit dem oben angesetzten „+“ Zeichen der Modul (der Elemente) des Ringes bezeichnet wird. Mit anderen Worten besagt ($\mathfrak{A}$), daß der Modul R^+ in die direkte Summe der Moduln A^+ und B^+ zerlegt ist. Bekanntlich ist dabei der Ring R selbst dann und nur dann in die direkte Summe von A und B zerlegt, wofür wir $R = A + B$ schreiben, wenn A und B sogar Ideale von R sind. Gibt es eine direkte Zerlegung $R = A + B$ mit $A \neq 0$, $B \neq 0$, so nennt man R bekanntlich direkt zerlegbar. Im obigen allgemeineren Fall ($\mathfrak{A}$) sprechen wir von einer *(allgemeinen) Zerlegung* von R (in die Summe der Unterringe A, B) und gebrauchen hierfür die Bezeichnung

$$(\mathfrak{B}) \qquad R = A \dotplus B.$$

Wenn für R mindestens eine Zerlegung ($\mathfrak{B}$) mit $A \neq 0$, $B \neq 0$ existiert, so nennen wir R einen *zerlegbaren* Ring.

Ein einfaches Beispiel für eine (nicht direkte) Zerlegung von Ringen geben wir hier an, einige weniger triviale Beispiele folgen in § 2.

Es sei R ein Matrizenring von endlichem Rang. Wir betrachten zuerst die Matrizen in R, in denen unterhalb der Diagonale alle Elemente gleich 0, dann die Matrizen, in denen die übrigen Elemente gleich 0 sind. Diese Matrizen bilden in R je einen Unterring A bzw. B mit $R = A \dotplus B$ und dabei ist weder A noch B ein Ideal von R, also ist $R \neq A + B$.

Wir wollen uns mit dem entsprechenden inversen Problem beschäftigen, das wir folgenderweise formulieren:

Zu beliebigen Ringen A, B sind diejenigen Ringe R zu bestimmen, für die

$$(\mathfrak{C}) \qquad R = A' \dotplus B', \; A' \cap B' = 0, \; A' \approx A, \; B' \approx B$$

gelten, wobei $\approx$ die Isomorphie bezeichnet. Wir sagen dann, dass der Ring R aus den Ringen A und B durch *(allgemeine) Zusammensetzung* entsteht.

Dabei handelt es sich also um eine Verallgemeinerung der direkten Zusammensetzung von Ringen und auch von den zerfallenden Everettschen Ringerweiterungen (vgl. EVERETT [2], RÉDEI [7]).

Aus ($\mathfrak{C}$) entsteht nach Einbettung von A und B der obigen Fall ($\mathfrak{B}$). (Hieraus sieht man, dass es sich bei ($\mathfrak{C}$) um eine Art Erweiterungsproblem handelt, wobei nämlich nach einem gemeinsamen Erweiterungsring von A und B gefragt wird.) Wegen des Gesagten schreiben wir auch im Fall ($\mathfrak{C}$) einfach $R = A \dotplus B$ (wie bei ($\mathfrak{B}$)), wenn daraus kein Mißverständnis entsteht.

Eine „explizite" Lösung unseres Problems ist freilich unvorstellbar, aber wir werden es im Satz 1 in einem ähnlichen Sinne allgemein lösen, wie das z. B. in der Everettschen Ringerweiterungstheorie zu meinen ist Aus Satz 1 ziehen wir dann gewisse Schlüße allgemeiner Natur bezüglich der Eigenschaften unserer Ringe (Sätze 2, 3, 4). Außerdem konnten wir einige Feststellungen von spezieller Natur erzielen, die uns ebenfalls interessant zu sein scheinen (Sätze 5 bis 8).

Freilich ließen sich in unserem Problemkreis mehrere weitere Fragen stellen. Es ist z. B. eine interessante Frage, die wir aber nicht beantworten konnten, ob es unter unserem Ringen $R = A \dotplus B$ auch einfache Ringe (insbesondere Schiefkörper) gibt.

Es ist klar, dass sich unser Problem mit entsprechender Änderung allgemeiner für beliebige „gleichartige" Strukturen formulieren läßt, wobei man immer unter den in diesen Strukturen erklärten Verknüpfungen eine auszeichnet (in unserem obigen Fall, wo es sich um Ringe handelt, haben wir ja die Addition ausgezeichnet). Im Fall von Strukturen mit einer Verknüpfung (z. B. Gruppen oder Halbgruppen) ist eine solche Auszeichnung freilich nicht nötig.

Insbesondere für Gruppen lautet also dieses Erweiterungsproblem folgenderweise:

Es seien G und Γ zwei beliebige Gruppen. Es sind die sämtlichen Gruppen $\mathfrak{G}$ mit

$$\mathfrak{G} = G'\Gamma', \quad G' \cap \Gamma' = 1, \quad G' \approx G, \quad \Gamma' \approx \Gamma$$

zu bestimmen.

Der Leser sieht, daß es sich eben um das bekannte Problem der Gruppenfaktorisation (oder nach einer neulich von B. H. NEUMANN eingeführten Terminologie um das allgemeine Gruppenprodukt) handelt. Dieses gruppentheoretische Problem gab in den letzten Jahren zu vielen wichtigen Untersuchungen Anlaß. Eben diese Untersuchungen haben uns an unser ringtheoretisches Problem geleitet.

Dem geschilderten Umstand entsprechend weist ein Teil unserer Resultate eine Ähnlichkeit mit Sätzen aus der Theorie der Gruppenfaktorisation auf. Auf diese Analogien werden wir in Fußanmerkungen jedesmal hinweisen.

§ 2. Beispiele.[1])

Um das Interesse für unser Problem zu erwecken, erwähnen wir hier noch einige Beispiele.

1. Es sei $w_1, w_2, \ldots, w_1', w_2', \ldots$ die Basis eines Ringes R (d. h. seines Moduls R^+) mit $w_i w_k = w_{i+k}$, $w_i' w_k' = w_{i+k}'$, $w_i' w_k = w_{i+k}$, $w_i w_k' = w_{i+k}'$. Die $w_1, w_2, \ldots$ bzw. $w_1', w_2', \ldots$ erzeugen in R einen Unterring A bzw. B mit $R = A \dotplus B$. Diese Unterringe A und B sind in R Linksideale (aber keine Rechtsideale).

2. Wir betrachten zwei Polynomringe $R[x]$, $R[y]$ über einem Ring R und bezeichnen mit $R_0[x]$, $R_0[y]$ ihre Unterringe bestehend aus den durch x bzw. y teilbaren Polynomen. In der direkten Summe $R_0[x]^+ + R_0[y]^+$ definieren wir eine Multiplikation der Elemente durch

$$(f_1(x)+g_1(y))(f_2(x)+g_2(y)) = f_1(x)f_2(x)+g_1(x)f_2(x)+f_1(y)g_2(y)+g_1(y)g_2(y).$$

So entsteht ein Ring $R_0[x] \dotplus R_0[y]$. In diesem sind $R_0[x]$, $R_0[y]$ Linksideale.

3. Es seien R_1, R_2 zwei isomorphe Ringe, die nur 0 als gemeinsames Element enthalten. Dann sind auch die Polynomringe $R_1[x]$, $R_2[y]$ isomorph und haben nur das Element 0 gemeinsam. Mit $f_1(x)$, $f_2(y)$ (oder $g_1(x)$, $g_2(y)$ usw.) bezeichnen wir stets zwei einander isomorph zugeordnete Polynome. In der direkten Summe $R_1[x]^+ + R_2[y]^+$ definieren wir eine Multiplikation durch

$$(f_1(x)+g_2(y))(h_1(x)+k_2(y)) = f_1(x)h_1(x)+g_1(x)h_1(x)+f_2(y)k_2(y)+g_2(y)k_2(y).$$

So entsteht ein Ring $R_1[x] \dotplus R_2[y]$. In diesem sind $R_1[x]$, $R_2[y]$ Linksideale.

4. Es sei K ein Körper von der Primzahlcharakteristik p. Mit K_x und K_y bezeichnen wir die Unterringe von $K[x]$ und $K[y]$ bestehend aus den (lückenhaften) Polynomen von der Form $\Sigma a_i x^{p^i}$ bzw. $\Sigma a_i y^{p^i}$. In der direkten Summe $K_x^+ + K_y^+$ werde die Multiplikation definiert:

$$(f(x)+g(y))(h(x)+k(y)) = f(h(x))+g(h(x))+f(k(y))+g(k(y)).$$

Der Leser sieht leicht (vgl. ORE [5]), daß hierdurch ein Ring entstanden ist, in dem K_x und K_y Linksideale sind.

---

[1]) Die Beispiele 2), 3), 4) und das in der Einleitung erwähnte verdanke ich Herrn Professor RÉDEI.

5. Es sei $w_1, w_2, \ldots, w_1', w_2', \ldots$ die Basis eines Ringes R mit $w_i w_k = w_i' w_k' = 0$, $w_i w_k' = w_k' w_i = (i+k)(w_1 + w_1')$ $(i, k \neq 1)$, $w_i w_1' = w_1' w_i = w_i' w_1 = w_1 w_i' = 0$. Die Basiselemente $w_1, w_2, \ldots$ bzw. $w_1', w_2', \ldots$ erzeugen in R einen Unterring A bzw. B mit $A \dotplus B$. Abweichend von den vorigen Beispielen ist jetzt weder A noch B ein einseitiges Ideal von $A \dotplus B$ (ähnliches bezieht sich auf das in der Einleitung angegebene Beispiel).

§ 3. Die Lösung des Problems.

Unser Erweiterungsproblem läßt sich ohne Einschränkung der Allgemeinheit so formulieren:

Es sind zu gegebenen Ringen A $(\neq 0)$ und $B(\neq 0)$ mit $A \cap B = 0$ die Ringe

(1) $$R = A \dotplus B$$

zu bestimmen.

Zur Lösung des Problems definieren wir R^+ (anders als in § 1) als die direkte Summe der Moduln A^+ und B^+. Dann nehmen wir vier (eindeutige) Funktionen

(2) $$a^b,\ {}^b a\ (\in A);\quad b'',\ {}^a b\ (\in B)\qquad (a \in A, b \in B)$$

und definieren in R^+ die Multiplikation durch

(3) $$ab = a^b + {}^a b, \qquad ba = {}^b a + b^a$$

und

(4) $$(a+b)(a'+b') = aa' + ba' + ab' + bb' \qquad (a, a' \in A;\ b, b' \in B),$$

wobei aa' und bb' (selbstverständlich) Elementenprodukte in A bzw. B bedeuten.

Damit auf diesem Wege ein Ring entsteht, ist vor allem nötig, dass die Multiplikation eindeutig ist, was aber nach (2) und (3) insbesondere für die Produkte $0a, a0, 0b, b0$ wegen $0 \in A, B$ und $0a = a0 = 0b = b0 = 0$ erst durch

(5) $$a^0 = {}^0 a = 0^a = {}^a 0 = b^0 = {}^0 b = 0^{b'} = {}^{b'} 0 = 0$$

gesichert ist. Deshalb nehmen wir die Erfülltheit dieser „Anfangsbedingungen" (5) oft stillschweigend von vornherein an, aus denen die Eindeutigkeit der Multiplikation offenbar folgt.

Die aus R^+ so entstandene Struktur (mit zwei Verknüpfungen) bezeichnen wir mit R^*. Es ist klar, daß die unter den R^* vorkommenden Ringe eben die sämtlichen Lösungen unseres Problems sind. Hiernach fragt es sich nur noch danach, welchen Bedingungen die Funktionen (2) zu genügen haben, damit R^* ein Ring ist.

Satz 1. *Die soeben definierte Struktur R^* ist dann und nur dann ein Ring, wenn für $a, a' \in A$ und $b, b' \in B$ die folgenden Beziehungen gelten:*

$$(6)\qquad \begin{aligned} a^{b+b'} &= a^b + a^{b'}, & {}^{b+b'}a &= {}^ba + {}^{b'}a,\\ b^{a+a'} &= b^a + b^{a'}, & {}^{a+a'}b &= {}^ab + {}^{a'}b, \end{aligned}$$

$$(7)\qquad \begin{aligned} (a+a')^b &= a^b + a'^b, & {}^b(a+a') &= {}^ba + {}^ba,\\ (b+b')^a &= b^a + b'^a, & {}^a(b+b') &= {}^ab + {}^ab', \end{aligned}$$

$$(8)\qquad \begin{aligned} (a^b)^{b'} &= a^{bb'}, & {}^{b'}({}^ba) &= {}^{b'b}a,\\ (b^a)^{a'} &= b^{aa'}, & {}^{a'}({}^ab) &= {}^{a'a}b, \end{aligned}$$

$$(9)\qquad \begin{aligned} (aa')^b &= aa'^b + a^{a'b}, & {}^b(aa') &= {}^baa' + {}^{b^a}a',\\ (bb')^a &= bb'^a + b^{b'a}, & {}^a(bb') &= {}^abb' + {}^{a^b}b', \end{aligned}$$

$$(10)\qquad (a^b)a' + {}^{a^b}a' = a^{ba'} + a({}^ba'), \qquad (b^a)b' + {}^{b^a}b' = b^{ab'} + b({}^ab'),$$

$$(11)\qquad ({}^ba)^{b'} = {}^b(a^{b'}), \qquad ({}^ab)^{a'} = {}^a(b^{a'}).$$

Und zwar sind die so entstehenden Ringe eben die sämtlichen Ringe R mit der Eigenschaft (1).[1])

Beweis. Wir brauchen nach Obigen nur die Behauptung „dann und nur dann" zu beweisen.

Damit R ein Ring ist, ist notwendig und hinreichend, daß die Multiplikation in R assoziativ und distributiv ist.

Da A und B Ringe sind, so sind für die Distributivität die Bedingungen

$$(12)\qquad \begin{aligned} &(a+a')b = ab + a'b,\ b(a+a') = ba + ba',\\ &a(b+b') = ab + ab',\ (b+b')a = ba + b'a \end{aligned}$$

notwendig und hinreichend. Die Notwendigkeit ist nämlich trivial. Anderseits folgt aus (12) und (4) für beliebige drei Elemente $a+b, a'+b', a''+b''$ $(a, a', a'' \in A;\ b, b', b'' \in B)$ nach

$$\begin{aligned} [(a+b)+(a'+b')](a''+b'') &= [(a+a')+(b+b')](a''+b'') =\\ &= (a+a')a'' + (b+b')a'' + (a+a')b'' + (b+b')b'' =\\ &= aa' + a'a'' + ba'' + b'a'' + ab'' + a'b'' + bb'' + b'b'' =\\ &= (a+b)(a''+b'') + (a'+b')(a''+b'') \end{aligned}$$

die Rechtsdistributivität. Auf die Linksdistributivität schließt man ähnlich.

Nun kann (12) wegen (3) auch so geschrieben werden:

$$\begin{aligned} (a+a')^b + {}^{a+a'}b &= a^b + {}^ab + a'^b + {}^{a'}b,\\ b^{a+a'} + {}^b(a+a') &= b^a + {}^ba + b^{a'} + {}^ba',\\ a^{b+b'} + {}^a(b+b') &= a^b + {}^ab + a^{b'} + {}^ab',\\ (b+b')^a + {}^{b+b'}a &= b^a + {}^ba + b'^a + {}^{b'}a. \end{aligned}$$

[1]) Den entsprechenden Satz für Gruppen samt Verallgemeinerungen s. in den Arbeiten [1], [6], [8], [11].

Diese vier Gleichungen sind wegen $A \cap B = 0$ gleichbedeutend mit den Gleichungen (6) und (7), also drücken diese letzteren genau die notwendige und hinreichende Bedingung der Distributivität aus. Im folgenden können wir die Gleichungen (6) und (7) schon voraussetzen.

Da A und B Ringe sind, so drücken (wegen der angenommenen Distributivität)

$$(13)\quad (aa')\,b = a(a'b),\ b(aa') = (ba)\,a',\ (bb')\,a = b(b'a),\ a(bb') = (ab)\,b',$$

$$(14)\quad (ab)\,a' = a(ba'),\ (ba)\,b' = b(ab')$$

offenbar die notwendige und hinreichende Bedingung der Assoziativität der Multiplikation aus. Da nach (3)

$$(aa')\,b = (aa')^b + {}^{aa'}b;\ a(a'b) = a(a'^b + {}^{a'}b) = aa'^b + a({}^{a'}b) = aa'^b + a^{a'^b} + {}^a({}^{a'}b),$$
$$b(aa') = b^{aa'} + {}^b(aa');\ (ba)\,a' = (b^a + {}^ba)\,a' = (b^a)\,a' + {}^baa' = (b^a)^{a'} + {}^{b^a}a' + {}^baa',$$
$$(bb')\,a = (bb')^a + {}^{bb'}a;\ b(b'a) = b(b'^a + {}^{b'}a) = bb'^a + b({}^{b'}a) = bb'^a + b^{b'^a} + {}^b({}^{b'}a),$$
$$a(bb') = a^{bb'} + {}^a(bb');\ (ab)\,b' = (a^b + {}^ab)\,b' = (a^b)\,b' + {}^abb' = (a^b)^{b'} + {}^{a^b}b' + {}^abb'$$

gelten, so ist (13) wegen $A \cap B = 0$ äquivalent mit den Gleichungen (8), (9).

Aus (3) folgen ferner

$$(ab)\,a' = (a^b + {}^ab)\,a' = (a^b)\,a' + {}^aba' = (a^b)\,a' + ({}^ab)^{a'} + {}^{a^b}a',$$
$$a(ba') = a(b^{a'} + {}^ba') = ab^a + a({}^ba') = a^{b^{a'}} + {}^a(b^{a'}) + a({}^ba'),$$
$$(ba)\,b' = (b^a + {}^ba)\,b' = (b^a)\,b' + {}^bab' = (b^a)\,b' + ({}^ba)^{b'} + {}^{b^a}b',$$
$$b(ab') = b(a^{b'} + {}^ab') = ba^{b'} + b({}^ab') = b^{a^{b'}} + {}^b(a^{b'}) + b({}^ab')$$

also ist (14) äquivalent mit den Gleichungen (10), (11). Somit haben wir den Satz bewiesen.

Wir nennen einen Funktionenvierer (2) *gut*, wenn für diesen die Bedingungen (5)—(11) erfüllt sind, und nennen eine der vier Funktionen (2) gut, wenn sie in einen guten Funktionenvierer gehört.

§ 4. Weitere Eigenschaften.

Die Relationen (7) zeigen, daß sich jedem Element b von B bzw. zu jedem Element a von A je zwei Endomorphismen von A^+ bzw. B^+ zuordnen lassen. Diese vier Endomorphismen sind nämlich die folgenden:

$$a \to a^b,\quad a \to {}^ba,\quad b \to {}^ab,\quad b \to b^a,$$

wobei das Zeichen „$\to$“ zur Bezeichnung der Abbildung dient.

Wir bezeichnen diese Endomorphismen mit A^b, ${}^bA$, ${}^aB$, B^a. Für ihre Addition und Multiplikation gelten nach (7) und (9) bzw. die folgenden

$$A^b + A^{b'} = A^{b+b'}, \qquad {}^bA + {}^{b'}A = {}^{b+b'}A, \tag{15}$$

$$A^{b'}A^b = A^{bb'}, \qquad {}^bA\,{}^{b'}A = {}^{bb'}A, \tag{16}$$

$$B^a + B^{a'} = B^{a+a'}, \qquad {}^aB + {}^{a'}B = {}^{a+a'}B, \tag{17}$$

$$B^{a'}B^a = B^{aa'}, \qquad {}^aB\,{}^{a'}B = {}^{aa'}B. \tag{18}$$

Da B ein Ring ist, sieht man hieraus, dass (15_1) und (16_1) einen zu B antihomomorphen Ring, (15_2) und (16_2) einen zu B homomorphen Ring definieren. Wir bezeichnen diese Ringe mit A^B bzw. ${}^BA$. Entsprechend definieren wir auf Grund von (17) und (18) die Ringe B^A und ${}^AB$. Es gilt also der folgende

Satz 2. *In jedem Ring $R = A + B$ bestehen*

$$B \tilde{a} A^B, \quad B \sim {}^BA, \quad A \tilde{a} B^A, \quad A \sim {}^AB,$$

wobei $\sim$ und $\tilde{a}$ die Homomorphie bzw. die Antihomomorphie bezeichnet.[1])

Wir bezeichnen den Kern des Homomorphismus $A \sim {}^AB$ bzw. $B \sim {}^BA$ mit

$$^\circ A \text{ bzw. } {}^\circ B \tag{19}$$

und den Kern des Antihomomorphismus $A \tilde{a} B^A$ bzw. $B \tilde{a} A^B$ mit

$$A^\circ \text{ bzw. } B^\circ. \tag{20}$$

Wir betrachten jetzt z. B. den Ring ${}^\circ A$ (d. h. die Menge derjenigen Elemente a, für die ${}^aB = 0$ ist). Aus (4) sehen wir, daß für jedes Element a von A und b von B $ab = a^b$ $(\in A)$ ist. Nach ${}^aB = 0$ folgt aus (9) ${}^{a^b}b' = 0 (b' \in B)$, also ${}^{a^b}B = 0$, d. h. $a^b \in {}^\circ A$. Somit gilt

$$^\circ AB \subseteq {}^\circ A. \tag{21}$$

Ähnlich läßt sich für A°

$$BA^\circ \subseteq A \tag{22}$$

zeigen. Ferner entstehen für den Ring ${}^\circ B$ bzw. B°

$$^\circ BA \subseteq {}^\circ B, \tag{23}$$

$$AB^\circ \subseteq B^\circ. \tag{24}$$

Da ${}^\circ A$, A° Ideale in A, und ${}^\circ B$, B° Ideale in B sind, so folgt

Satz 3. *In $R = A + B$ ist A° ein Linksideal, ${}^\circ A$ ein Rechtsideal, B° ein Linksideal, ${}^\circ B$ ein Rechtsideal.*

Wenn $\bar{A} \subseteq A$ ein Linksideal in R ist, dann ist offenbar $B^{\bar{a}} = 0 (\bar{a} \in \bar{A})$. Ähnlich, wenn $\bar{\bar{A}} \subseteq A$ ein Rechtsideal in R ist, so ist ${}^{\bar{\bar{a}}}B = 0$ $(\bar{\bar{a}} \in \bar{\bar{A}})$, wenn ferner $\bar{B} \subseteq B$ ein Linksideal in R ist, so ist $A^{\bar{b}} = 0$ $(\bar{b} \in \bar{B})$, wenn endlich

[1]) Den analogen Satz im Fall der Gruppen s. [9], [10].

$\bar{\bar{B}} \subseteqq B$ ein Rechtsideal in R ist, so ist ${}^{\bar{b}}A = 0$ $(\bar{\bar{b}} \in \bar{\bar{B}})$. Daraus ergibt sich der folgende

Satz 4. *In einem Ring $R = A \dotplus B$ gelten: Das Linksideal A° enthält jedes Linksideal $\bar{A} \subseteqq A$ von R, das Rechtsideal ${}^\circ A$ von R enthält jedes Rechtsideal $\bar{\bar{A}} \subseteqq A$ von R, das Linksideal B° von R enthält jedes Linksideal $\bar{B} \subseteqq B$ von R, das Rechtsideal ${}^\circ B$ von R enthält jedes Rechtsideal $\bar{\bar{B}} \subseteqq B$ von R.*[1])

Bemerkung. In einem Ring $R = A \dotplus B$ ist A dann und nur dann ein Linksideal, wenn $B^A = 0$, d. h.

$$b^a = 0 \qquad (a \in A,\ b \in B).$$

Ferner ist A in R dann und nur dann ein Rechtsideal, wenn ${}^A B = 0$, d. h.

$${}^a b = 0 \qquad (a \in A,\ b \in B).$$

Ähnlich läßt sich entscheiden ob B ein Links- bzw. Rechtsideal in R ist.

Beispiel. Aus zwei isomorphen Ringen A und B wollen wir Ringe $R = A \dotplus B$ konstruieren, in denen A und B Linksideale sind. Die Elemente von A und B bezeichnen wir mit $a_1, a_2, \ldots$ bzw. $b_1, b_2, \ldots$, so daß

$$a_i \longleftrightarrow b_i$$

ein Isomorphismus zwischen A und B ist. Nach der vorigen Bemerkung müssen

$$b_i^{a_k} = a_i^{b_k} = 0 \qquad (i, k = 1, 2, \ldots)$$

gelten. Außerdem setzen wir

$${}^{a_i}b_k = b_i b_k, \quad {}^{b_i}a_k = a_i a_k.$$

Aus (3) und (4) ist klar, daß durch diese vier Funktionen nur Ringe der verlangten Art entstehen, aber es ist noch zu zeigen, daß die Bedingungen von Satz 1 erfüllt sind. Das sieht man einfach aus den folgenden Rechnungen

$$\begin{aligned}
&a_i^{b_k+b_l} = 0 = a_i^{b_k} + a_i^{b_l}, \quad b_i^{a_k+a_l} = 0 = b_i^{a_k} + b_i^{a_l},\\
(6')\qquad &{}^{b_k+b_l}a_i = (a_k + a_i)\, a_i = a_k a_i + a_l a_i = {}^{b_k}a_i + {}^{b_l}a_i,\\
&{}^{a_k+a_l}b_i = (b_k + b_l)\, b_i = b_k b_i + b_l b_i = {}^{a_k}b_i + {}^{a_l}b_i,
\end{aligned}$$

$$\begin{aligned}
&(a_k + a_l)^{b_i} = 0 = a_k^{b_i} + a_l^{b_i}, \quad (b_k + b_l)^{a_i} = 0 = b_k^{a_i} + b_l^{a_i},\\
(7')\qquad &{}^{b_i}(a_k + a_l) = a_i (a_k + a_l) = a_i a_k + a_i a_l = {}^{b_i}a_k + {}^{b_i}a_l,\\
&{}^{a_i}(b_k + b_l) = b_i (b_k + b_l) = b_i b_k + b_i b_l = {}^{a_i}b_k + {}^{a_i}b_l,
\end{aligned}$$

$$\begin{aligned}
&(a_i^{b_k})^{b_l} = 0 = a^{b_k b_l}, \quad (b_i^{a_k})^{a_l} = 0 = b_i^{a_k a_l},\\
(8')\qquad &{}^{b_l}({}^{b_k}a_i) = {}^{b_l}(a_k a_i) = a_l a_k a_i = {}^{b_l b_k}a_i,\\
&{}^{a_l}({}^{a_k}b_i) = {}^{a_l}(b_k b_i) = b_l b_k b_i = {}^{a_l a_k}b_i,
\end{aligned}$$

[1]) Den analogen Satz für Gruppen s. [9], [10].

$$(a_k a_l)^{b_i} = 0 = a_k a_l^{b_i} + a_k^{a_l b_i}, \quad (b_k b_l)^{a_i} = 0 = b_k b_l^{a_i} + b_k^{b_l a_i},$$

$$^{b_i}(a_k a_l) = a_i a_k a_l = {}^{b_i}a_k a_l + 0 = {}^{b_i}a_k a_l + {}^{b_i a_k}a_l, \tag{9'}$$

$$^{a_i}(b_k b_l) = b_i b_k b_l = {}^{a_i}b_k b_l + 0 = {}^{a_i}b_k b_l + {}^{a_i b_k}b_l,$$

$$(a_k^{b_i}) a_l + {}^{a_k b_i}a_l = {}^{b_k b_i}a_l = a_k a_i a_l = a_k({}^{b_i}a_l) + 0 = a_k({}^{b_i}a_l) + a_k^{b_i a_l}, \tag{10'}$$

$$(b_k^{a_i}) b_l + {}^{b_k a_i}a_l = {}^{a_k a_i}b_l = b_k b_i b_l = b_k({}^{a_i}b_l) + 0 = b_k({}^{a_i}b_l) + b_k^{a_i b_l}$$

$$({}^{b_k}a_i)^{b_l} = 0 = {}^{b_k}(a_i^{b_l}), \quad ({}^{a_k}b_i)^{a_l} = 0 = {}^{a_k}(b_i^{a_l}). \tag{11'}$$

Wir betrachten die Elemente $a(\in A)$ so beschaffen, daß $a^b = 0$ für alle Elemente b von B stattlhat. Diese a bilden einen Ring, denn aus $a^b = 0$ und $a'^b = 0$ folgt $(a+a')^b = a^b + a'^b = 0$, ferner ist auch $(aa')^b = aa'^b + a^{a'b} = 0$ erfüllt. Wir bezeichnen diesen Ring mit A_B. Da für jedes $a(\in A_B)$ und jedes $b(\in B)$ $ab = a^b + {}^a b(\in B)$ ist, so folgt $A_B B \subseteq B$. Umgekehrt, wenn $aB \subseteq B$ $(a \in A)$ ist, dann besteht $a^b = 0$ für jedes $b(\in B)$, d. h. es ist $a \in A_B$. Entsprechend können wir die Unterringe ${}_B A, B_A, {}_A B$ definieren. Nach vorigem gilt dann der

Satz 5. *In einem Ring $R = A \dotplus B$ sind A_B bzw. B_A die maximalen Unterringe $(\subseteq A)$, für die*

$$A_B B \subseteq B \quad \text{bzw.} \quad B\,{}_B A \subseteq B$$

gilt, ferner sind B_A bzw. ${}_A B$ die maximalen Unterringe $(\subseteq B)$, für die

$$B_A A \subseteq A \quad \text{bzw.} \quad A\,{}_A B \subseteq A.$$

Bemerkung. Es ist leicht zu sehen, daß der durch die Produkte $ab(a \in A_B, b \in B)$ erzeugte Modul $\{A_B B\}$ ein Rechtsideal in B ist. Einerseits ist nämlich $\{A_B B\}$ wegen

$$(ab)(a'b') = (ab)b'' = a(bb'') \in A_B B \qquad (a' \in A_B;\ b', b'' \in B)$$

ein Ring, andererseits ist offenbar

$$\{A_B B\} B \subseteq \{A_B B\}.$$

Eine entsprechende Behauptung gilt für die ähnlich erklärten Moduln $\{B\,{}_B A\}$, $\{A\,B_A\}$, $\{{}_A B\,A\}$.

Freilich sind die Bedingungen (6)—(11) voneinander abhängig. Unsere Aufgabe wird jetzt solche Abhängigkeiten zu untersuchen.

Satz 6. *Wenn die Werte von irgendwelchen Funktionen* (2) *mit der Eigenschaft* (5) *für die Generatoren der Moduln A^+ und B^+ angegeben sind, so sind diese Funktionen durch die Forderungen* (6), (7) *vollständig bestimmt. Sind dabei die Bedingungen* (8)—(11) *für die Generatoren von A^+ und B^+ erfüllt, so bestehen diese Bedingungen auch schon für alle Elemente von A und B.*

Beweis. Den Beweis fangen wir mit der einfachen Bemerkung an, daß die genannten Funktionen im Falle des Bestehens von (6), (7) so beschaffen sein müssen, daß sie nur eine Vorzeichenänderung erleiden, wenn in ihnen a oder b durch $-a$ bzw. $-b$ ersetzt wird. Hiervon genügt es z. B. $(-a)^b = -a^b$ zu beweisen, denn die übrigen Fälle sind ähnlich. Der Beweis entsteht sofort aus (7_1) bei Anwendung auf $a' = -a$, da dann die linke Seite nach (5) gleich 0 ist. Im Besitz dieser Bemerkung folgt die erste Hälfte des Satzes durch eine leichte Induktion.

Um die zweite Hälfte des Satzes zu beweisen, nehmen wir an, daß die Bedingungen (8) bis (11) für die Elemente $\bar{b}, \bar{\bar{b}} (\in B)$ und $\bar{a}, \bar{\bar{a}} (\in A)$ an Stelle von b oder b' bzw. a oder a' erfüllt sind. Aus

$$(a^{\bar{b}})^{b'} = a^{\bar{b}b'} \quad \text{und} \quad (a^{\bar{\bar{b}}})^{b'} = a^{\bar{\bar{b}}b'}$$

folgt nach (6) und (7)

$$(a^{\bar{b}+\bar{\bar{b}}})^{b'} = (a^{\bar{b}} + a^{\bar{\bar{b}}})^{b'} = (a^{\bar{b}})^{b'} + (a^{\bar{\bar{b}}})^{b'} = a^{\bar{b}b'} + a^{\bar{\bar{b}}b'} = a^{\bar{b}b'+\bar{\bar{b}}b'} = a^{(\bar{b}+\bar{\bar{b}})b'}.$$

Ähnlich bekommt man $(a^b)^{(\bar{b}+\bar{\bar{b}})} = a^{b(\bar{b}+\bar{\bar{b}})}$ und $((\bar{a}+\bar{\bar{a}})^b)^{b'} = (\bar{a}+\bar{\bar{a}})^{bb'}$. Das bedeutet das Bestehen von (8_1). Mit ($8_{2,3,4}$) verfährt man ähnlich.

Sind

$$(aa')^{\bar{b}} = aa'^{\bar{b}} + a^{a'\bar{b}}, \quad (aa')^{\bar{\bar{b}}} = aa'^{\bar{\bar{b}}} + a^{a'\bar{\bar{b}}}$$

gültig, so gilt nach (6) und (7)

$$(aa')^{\bar{b}+\bar{\bar{b}}} = (aa')^{\bar{b}} + (aa')^{\bar{\bar{b}}} = (aa')^{\bar{b}} + a^{a'\bar{b}} + aa'^{\bar{\bar{b}}} + a^{a'\bar{\bar{b}}} =$$
$$= a(a'^{\bar{b}} + a'^{\bar{\bar{b}}}) + a^{a'\bar{b}+a'\bar{\bar{b}}} = aa'^{\bar{b}+\bar{\bar{b}}} + a^{a'(\bar{b}+\bar{\bar{b}})}.$$

Das beweist einen Teil der Behauptung über (9_1).

Hieraus sieht man leicht wie der Beweis von Satz 6 weiter auszuführen ist.

Es seien die Ringe A und B gegeben. Es gilt der folgende

Satz 6.[1]) *Ist a^b eine gute Funktion ($a \in A$, $b \in B$), so determiniert a^b die Funktionswerte von "b mod B°. Eine gute Funktion ^ba determiniert die Funktionswerte von b" mod °B. Eine gute Funktion "b determiniert die Funktionswerte von a^b mod A°. Endlich determiniert eine gute Funktion b" die Funktionswerte von ^ba mod °A.*

Beweis. Es folgt aus (9_1)

$$a'^{a_b} = (a'a)^b - a'a^b. \tag{26}$$

Hiernach haben für gegebene a und b sämtliche Gleichungen

$$a'^{b^*} = (a'a)^b - a'a^b \tag{26}$$

je eine Lösung b^* ($a' \in A$, $b^* \in B$).

[1]) Den analogen Satz für Gruppen (in einem speziellen Fall) s. [6].

Wir zeigen, daß zwei Lösungen $b_1^*, b_2^* (\in B)$ von (26) zu derselben Restklasse mod B° gehören. Für b_1^*, b_2^* gelten nämlich,

$$a'^{b_1^*} = a'^{b_2^*}$$

also gilt wegen (6)

$$a'^{b_1^* - b_2^*} = 0$$

für jedes $a' \in A$. Somit gilt

$$b_1^* - b_2^* \in B^\circ$$

Da ferner nach (25) ${}^{a}b$ eine Lösung von (26) ist, so ist hiermit die erste Behauptung von Satz 6 bewiesen.

Die übrigen Behauptungen beweist man ähnlich.

Bemerkung. Gilt im Satz 6 insbesondere $B^\circ = 0$ bzw. ${}^\circ B = 0$, so ist die Funktion ${}^{a}b$ bzw. b^{a} durch die Funktion a^b bzw. ${}^b a$ sogar eindeutig bestimmt. Entsprechendes gilt für die Funktionen ${}^b a$, a^b in den Fällen $A^\circ = 0$ und ${}^\circ A = 0$.

Für ein beliebiges Ideal des zerlegbaren Ringes R gilt der folgende

Satz 7. *Ist $\mathfrak{a}$ ein Ideal von $R = A + B$ bestehend aus den Elementen $a_1 + b_1, a_2 + b_2, \ldots$ $(a_i \in A, b_i \in B, i = 1, 2, \ldots)$, so bilden die a_i bzw. b_i Unterringe A' bzw. B' von R, ferner ist $R' = A'^+ + B'^+$ ein (zerlegbarer) Unterring von R mit $R' = A' + B'$, für den $\mathfrak{a} \subseteq R'$ besteht.*

Beweis. Da $(a_i + b_i) + (a_j + b_j) = (a_i + a_j) + (b_i + b_j) \in \mathfrak{a}$ ist, so bilden die Elemente a_i bzw. b_i gewisse Moduln A' bzw. B'. Für beliebige Elemente a $(\in A)$ und $a_i + b_i$ $(\in \mathfrak{a})$ ist

$$a(a_i + b_i) = aa_i + ab_i = aa_i + a^{b_i} + {}^{a}b_i \qquad (\in \mathfrak{a}), \tag{27}$$

woraus ${}^{a}b_i \in B'$ folgt. Ähnlich folgt aus

$$(a_i + b_i)a = a_i a + b_i^{a} + {}^{b_i}a \quad (\in \mathfrak{a}) \tag{28}$$

$b_i^a \in B'$. Auf demselben Weg können wir a_i^b, ${}^b a_i \in A'$ $(b \in B)$ zeigen. Aus der Relation

$$(a_i + b_i)a_k = a_i a_k + b_i^{a_k} + {}^{b_i}a_k \quad (\in \mathfrak{a}) \tag{29}$$

folgt $a_i a_k + {}^{b_i}a_k \in A'$, und daraus $a_i a_k \in A'$. Auf dieselbe Weise folgt $b_i b_k \in B'$. Also sind A' und B' Unterringe von A bzw. B.

Wir betrachten die Summe $A'^+ + B'^+$, die also ein Untermodul von R ist. Auf Grund der vorher Bewiesenen ist

$$a_k(a_l + b_l) = a_k a_l + a_k^{b_l} + {}^{a_k}b_l \in A'^+ + B'^+ \tag{30}$$

d. h. $A'(A'^+ + B'^+) \subseteq A'^+ + B'^+$. Ähnlich ist

$$(A'^+ + B'^+)A', \quad B'(A'^+ + B'^+), \quad (A'^+ + B'^+)B' \subseteq A'^+ + B'^+$$

Hiernach ist der Modul $A'^+ + B'^+$ ein Ring. Die Behauptung $\mathfrak{a} \subseteq R'$ ist trivial.

In Verbindung mit den zerlegbaren Ringen $R = A \dotplus B$ entsteht die Frage, ob unter diesen Ringe auch Körper vorkommen. Auf dieses Problem bezieht sich der folgende

Satz 8. *Enthalten die Ringe* $A(\neq 0)$, $B(\neq 0)$ *je ein minimales Linksideal, so hat jeder Ring* $R = A \dotplus B$ *ein echtes Linksideal.*

Beweis. Nehmen wir an, daß der Satz falsch ist, d. h. R kein echtes Linksideal enthält. Da R kein Zeroring von Primzahlordnung ist, so folgt aus dem Struktursatz von WEDDERBURN—ARTIN leicht, daß R ein Schiefkörper sein muß. Da A und B nullteilerfrei sind, kann ihr Einselement (wenn es existiert) nur das von R sein. Da aber $A \cap B = 0$ ist, so folgt, daß mindestens das eine von A und B ohne Einselement ist.

Wir nehmen an, daß A kein Einselement hat, und betrachten das minimale Linksideal $\mathfrak{a}$ von A. Es sei a ein von 0 verschiedenes Element von $\mathfrak{a}$. Da $Aa(\neq 0)$ ein Linksideal von $A(\subseteq \mathfrak{a})$ ist, so ist $Aa = \mathfrak{a}$. Hieraus folgt die Existenz eines Elementes e von A mit $ea = a$. Da aber A keinen Nullteiler hat, so folgt hieraus, daß e sein Einselement ist. Dieser Widerspruch beweist den Satz.

Literaturverzeichnis.

[1] G. CASADIO, Costruzione di gruppi come prodotto di sottogruppi permutabili, *Rendiconti di mat. e delle sue applicazioni*, (V) **2** (1951), 348—360.

[2] C. J. EVERETT, An extension theory for rings, *American Journal of Math.*, **64** (1942), 363—370.

[3] L. FUCHS, Rédeian skew product of operator groups, *Acta Sci. Math.*, **14** (1952), 228—238.

[4] B. HUPPERT, Über Produkte von endlichen Gruppen, *Wiss. Zeitschrift der Humbolt-Univ. Berlin*, Nr. 5, Jahrgang III (1953—54).

[5] O. ORE, On a special class of polynomials, *Transactions American Math. Soc.*, **35** (1933), 559—584.

[6] L. RÉDEI, Die Anwendung des schiefen Produktes in der Gruppentheorie, *Journal für die reine und angew. Math.*, **188** (1950), 201—228.

[7] ———, Die Verallgemeinerung der Schreierschen Erweiterungstheorie, *Acta Sci. Math.*, **14** (1952), 252—273.

[8] L. RÉDEI und J. SZÉP, Die Verallgemeinerung der Theorie des Gruppenproduktes von Zappa—Casadio, *Acta Sci. Math.*, **16** (1955), 165—170.

[9] J. SZÉP, Über die als Produkt zweier Untergruppen darstellbaren endlichen Gruppen, *Commentarii Math. Helvetici*, **22** (1949), 31—33.

[10] J. SZÉP und L. RÉDEI, On factorisable groups, *Acta Sci. Math.*, **13** (1950), 235—238.

[11] G. ZAPPA, Sulla costruzione dei gruppi di due dati sottogruppi permutabili tra loro, *Atti 2. Congr. Unione Math. Ital.* (1942), 119—125.

(Eingegangen am 16. März 1957.)

Über eine allgemeine Ringkonstruktion durch schiefes Produkt.

Von J. SZENDREI in Szeged.

§ 1. Einleitung.

Das Prinzip des schiefen Produktes geht auf HAMILTON zurück und ist ein alltägliches Werkzeug der Algebra, um aus gegebenen Strukturen neue Strukturen zu konstruieren. In einer Arbeit [4][1]) hat L. RÉDEI einen sehr allgemeinen Typ von schiefen Produkten zweier Gruppen untersucht, der die Schreierschen Erweiterungen und die Zappa—Szépschen Produkte als Spezialfälle enthält. In einer anderen Arbeit [5] hat er zwei einfache Beispiele zur Konstruktion von Ringen betrachtet, die übrigens einander sehr ähneln. Mehrere Autoren haben schon auch bisher ihre Aufmerksamkeit auf die Theorie des schiefen Produktes in der Gruppentheorie berichtet. (Vgl. KOCHENDÖRFFER [3], RÉDEI und STÖHR [7], RÜHS [8].) Neulich hat G. SZÁSZ in seiner Arbeit [9] das schiefe Produkt von Halbverbänden untersucht.

In dieser Arbeit beschäftigen wir uns mit einem gewißen Typ von schiefem Produkt zweier Ringe. Dieser Typ ist sehr allgemein, und man kann ihn als das ringtheoretische Analogon des Rédeischen schiefen Produktes betrachten.

Stets sollen R, P zwei Ringe mit den Elementen $0, a, b, \ldots$ bzw. $o, \alpha, \beta, \ldots$ bezeichnen, wobei $0, o$ die Zeroelemente von R bzw. P sind. Wir betrachten die (geordneten) Paare

$$(a, \alpha) \qquad (a \in R,\ \alpha \in \mathsf{P}).$$

Das Element a und α heißt die R- bzw. P-*Komponente* von (a, α). Die Gleichheit der Elemente (a, α), (a', α') ist mit $a = a'$, $\alpha = \alpha'$ definiert. Die Menge dieser Paare machen wir zu einer Struktur, die wir mit $R \circ \mathsf{P}$ bezeichnen, so, daß wir die Addition und Multiplikation durch

$$(1) \qquad (a, \alpha) + (b, \beta) = (a + b + [\alpha, \beta], [a, b] + \alpha + \beta),$$

$$(2) \qquad (a, \alpha)(b, \beta) = (ab + a^{\beta} + {}^{\alpha}b + \{\alpha, \beta\}, \{a, b\} + \alpha^{b} + {}^{a}\beta + \alpha\beta)$$

[1]) Die Nummern in eckigen Klammern verweisen auf das Literaturverzeichnis am Ende der Arbeit.

definieren, wobei die Funktionen

$$[\alpha, \beta], \{\alpha, \beta\}, a^{\beta}, {}^{\alpha}b \in R; \quad [a, b], \{a, b\}, \alpha^{b}, {}^{\alpha}\beta \in \mathsf{P} \tag{3}$$

den Anfangsbedingungen

$$\begin{aligned} &[\alpha, o] = [o, \alpha] = \{\alpha, o\} = \{o, \alpha\} = 0^{\alpha} = a^{o} = {}^{\alpha}0 = {}^{o}a = 0, \\ &[a, 0] = [0, a] = \{a, 0\} = \{0, a\} = o^{a} = \alpha^{0} = {}^{a}o = {}^{0}\alpha = o \end{aligned} \tag{B}$$

unterworfen sind. Die vier Funktionen a^{β}, ${}^{\alpha}b$ $(\in R)$, α^{b}, ${}^{\alpha}\beta$ $(\in \mathsf{P})$ in (3) können wir als *„Operatorprodukte"* auffassen. In diesem Sinne ist P (bzw. R) gleichzeitig ein Rechts- und Linksoperatorbereich von R (bzw. P). (Aber diese Operationen werden von der sonst üblichen abweichen.)

Aus (1), (2) und (B) folgen

$$\begin{aligned} &(a, o) + (b, o) = (a + b, [a, b]), \qquad (0, \alpha) + (0, \beta) = ([\alpha, \beta], \alpha + \beta]), \\ &(a, o)(b, o) = (ab, \{a, b\}), \qquad (0, \alpha)(0, \beta) = (\{\alpha, \beta\}, \alpha\beta), \\ &(a, o)(0, \beta) = (a^{\beta}, {}^{a}\beta), \qquad (0, \alpha)(b, o) = ({}^{\alpha}b, \alpha^{b}). \end{aligned}$$

Diese und (1), (2) zeigen, daß das Funktionensystem (3) und das schiefe Produkt $R \circ \mathsf{P}$ einander gegenseitig eindeutig bestimmen.

Vor allem werden wir die Bedingungen aufstellen, unter denen das schiefe Produkt $R \circ \mathsf{P}$ ein Ring ist.

Wir nennen die Struktur $R \circ \mathsf{P}$ *k-fach ausgeartet,* wenn genau k der acht Relationen

$$\begin{aligned} &[\alpha, \beta] = 0, \ \{\alpha, \beta\} = 0, \ a^{\beta} = 0, \ {}^{\alpha}b = 0, \\ &[a, b] = o, \ \{a, b\} = o, \ \alpha^{b} = o, \ {}^{\alpha}\beta = o \end{aligned}$$

identisch gelten. Wenn $k = 0$ ist, so nennen wir $R \circ \mathsf{P}$ auch *nicht ausgeartet.* Im Falle $k = 8$ ist $R \circ \mathsf{P}$ die direkte Summe von R und P.

Was die k-fachen $(k \neq 0, 8)$ Ausartungen von $R \circ \mathsf{P}$ anbelangt, so gibt es unter ihnen viele wesentlich verschiedene. Wir werden aber nur die folgenden wichtigen Fälle erwähnen:

$$R \in \mathsf{P}: \quad \begin{aligned} &(a, \alpha) + (b, \beta) = (a + b, [a, b] + \alpha + \beta), \\ &(a, \alpha)(b, \beta) = (ab, \{a, b\} + \alpha^{b} + {}^{\alpha}\beta + \alpha\beta); \end{aligned} \tag{4}$$

$$R \subseteq \mathsf{P}: \quad \begin{aligned} &(a, \alpha) + (b, \beta) = (a + b, \alpha + \beta), \\ &(a, \alpha)(b, \beta) = (ab + a^{\beta} + {}^{\alpha}b, \alpha^{b} + {}^{\alpha}\beta + \alpha\beta); \end{aligned} \tag{5}$$

$$R * \mathsf{P}: \quad \begin{aligned} &(a, \alpha) + (b, \beta) = (a + b, \alpha + \beta), \\ &(a, \alpha)(b, \beta) = (ab + \{\alpha, \beta\}, \alpha^{b} + {}^{\alpha}\beta + \alpha\beta); \end{aligned} \tag{6}$$

$$R \bullet \mathsf{P}: \quad \begin{aligned} &(a, \alpha) + (b, \beta) = (a + b, \alpha + \beta), \\ &(a, \alpha)(b, \beta) = (ab, \alpha^{b} + {}^{\alpha}\beta + \alpha\beta). \end{aligned} \tag{7}$$

Die ersten zwei sind 4-fach ausgeartet. Es wird sich herausstellen, daß die Ringe $R \in \mathfrak{P}$ mit den Everettschen Erweiterungen [2], [6] von $\mathfrak{P}$ mit R zusammenfallen. Die Ringe $R \mathrm{s} \mathfrak{P}$ stimmen mit neulich von SZÉP [12] untersuchten Ringen überein. SZÉP hat über sie interessante Resultate erzielt.

Die Theorie von $R \circ \mathfrak{P}$ enthält also insbesondere die dem Wesen nach sehr verschiedenen Theorien von EVERETT und SZÉP.

Die Ringe $R * \mathfrak{P}$, die 5-fach ausgeartet sind, wurden bisher nicht betrachtet. Es wird gezeigt, daß diese Ringe die Konstruktion der komplexen Ringe und die der Quaternionenringe über einem Ring mit Einselement als Spezialfälle enthalten.[2]) Auf diese Weise kann man eine neue Konstruktion des Körpers der komplexen Zahlen und des Quaternionenkörpers angeben. Wir möchten betonen, daß unter den Ringkonstruktionen $R * \mathfrak{P}$ auch Körper vorkommen.

$R \bullet \mathfrak{P}$ ist einer der 6-fach ausgearteten Ringe, der als Spezialfall in $R \in \mathfrak{P}$, $R \mathrm{s} \mathfrak{P}$ und $R * \mathfrak{P}$ enthalten ist, und zwar handelt es sich im wesentlichen um die sogenannte faktorenfreie Everettsche Erweiterung [2], [6], [12]. Diese ist eine alltägliche und am frühesten eingeführte Ringkonstruktion (vgl. DORROH [1]).

Es ist uns nicht gelungen ein Beispiel für nichtausgeartete Ringe anzugeben.

§ 2. Die Ringe $R \circ \mathfrak{P}$.

Wir wollen in diesem Paragraphen notwendige und hinreichende Bedingungen aufstellen, damit ein schiefes Produkt $R \circ \mathfrak{P}$ von R und $\mathfrak{P}$ ein Ring ist.

Bevor wir den Satz 1 aussprechen, bemerken wir, daß man durch die Vertauschung der Elemente von R und $\mathfrak{P}$ in (1) und (2) aus der $R(\mathfrak{P})$-Komponente die $\mathfrak{P}(R)$ Komponente gewinnt. Folglich, wie es leicht zu sehen ist, liefert die Vertauschung der lateinischen und griechischen Buchstaben aus einer gültigen Formel in R ($\mathfrak{P}$), eine gültige Formel in $\mathfrak{P}$ (R), die wir die *duale* der ursprünglichen Formel nennen. Von zwei solchen Formeln genügt es also immer nur eine zu beweisen.

Wir beweisen nun den folgenden

---

[2]) Unter einem komplexen Ring über einem Ring R mit Einselement e verstehen wir nach RÉDEI die Menge der Elemente

$$a + bi \qquad (a, b \in R)$$

in der $ei = ie = i$, $i^2 = e$ gilt und die Addition und Multiplikation durch

$$(a + bi) + (c + di) = a + c + (b + d)i$$
$$(a + bi)(c + di) = ac - bd + (ad + bc)i$$

definiert werden.

Ähnlicherweise kann man den Quaternionenring über R definieren.

Satz 1. *Das durch* (1) *und* (2) *definierte schiefe Produkt mit den Anfangsbedingungen* (*B*) *ist dann und nur dann ein Ring, wenn*

$$(K) \qquad [\alpha, \beta] = [\beta, \alpha],$$

$$(A_1^+) \qquad [\alpha, \beta] + [\alpha + \beta, \gamma] = [\alpha, \beta + \gamma] + [\beta, \gamma],$$

$$(A_2^+) \qquad [[a, b], \gamma] = 0,$$

$$(A_1) \qquad a^{\{b,c\}} = {}^{\{a,b\}}c,$$

$$(A_2) \qquad {}^{\alpha}\{\beta, \gamma\} + \{\alpha, \beta\gamma\} = \{\alpha, \beta\}^{\gamma} + \{\alpha\beta, \gamma\},$$

$$(A_3) \qquad a({}^{\beta}c) + a^{({}^{\beta}c)} = (a^{\beta})c + {}^{(a^{\beta})}c,$$

$$(A_4) \qquad {}^{\alpha}(b^{\gamma}) + \{\alpha, {}^{b}\gamma\} = ({}^{\alpha}b)^{\gamma} + \{\alpha^{b}, \gamma\},$$

$$(A_5) \qquad a(b^{\gamma}) + a^{b^{\gamma}} = (ab)^{\gamma} + \{\{a, b\}, \gamma\}, \qquad ({}^{\alpha}b)c + {}^{\alpha^{b}}c = {}^{\alpha}(bc) + \{\alpha, \{b, c\}\},$$

$$(A_6) \qquad (a^{\beta})^{\gamma} + \{{}^{\alpha}\beta, \gamma\} = a^{\beta\gamma} + a\{\beta, \gamma\}, \qquad {}^{\alpha}({}^{\beta}c) + \{\alpha, \beta^{c}\} = {}^{\alpha\beta}c + \{\alpha, \beta\}c,$$

$$(D_1) \qquad \begin{aligned} {}^{\alpha}(b + c) + \{\alpha, [b, c]\} &= {}^{\alpha}b + {}^{\alpha}c + [\alpha^{b}, \alpha^{c}], \\ (a + b)^{\gamma} + \{[a, b], \gamma\} &= a^{\gamma} + b^{\gamma} + [{}^{a}\gamma, {}^{b}\gamma], \end{aligned}$$

$$(D_2) \qquad \begin{aligned} a^{\beta+\gamma} + a[\beta, \gamma] &= a^{\beta} + a^{\gamma} + [{}^{a}\beta, {}^{a}\gamma], \\ {}^{\alpha+\beta}c + [\alpha, \beta]c &= {}^{\alpha}c + {}^{\beta}c + [\alpha^{c}, \beta^{c}], \end{aligned}$$

$$(D_3) \qquad \begin{aligned} {}^{\alpha}[\beta, \gamma] + \{\alpha, \beta + \gamma\} &= \{\alpha, \beta\} + \{\alpha, \gamma\} + [\alpha\beta, \alpha\gamma], \\ [\alpha, \beta]^{\gamma} + \{\alpha + \beta, \gamma\} &= \{\alpha, \gamma\} + \{\beta, \gamma\} + \{\alpha\gamma, \beta\gamma\}, \end{aligned}$$

$$(D_4) \qquad a^{[b,c]} = [\{a, b\}, \{a, c\}], \qquad {}^{[a,b]}c = [\{a, c\}, \{b, c\}],$$

$$(D_5) \qquad [\{a, b\} + \alpha^{b}, {}^{a}\gamma + \alpha\gamma] = 0, \qquad [\{a, c\} + {}^{\alpha}\gamma, \beta^{c} + \beta\gamma] = 0$$

und die dualen Gleichungen gelten.

Bemerkung. Man kann leicht sehen, daß die additive Gruppe des Ringes $R \circ P$ die von RÉDEI [4] herrührende Gruppe $G^{3}\Gamma$ (im kommutativen Fall) ist. Dieser Typ wurde auch von KOCHENDÖRFFER [3] untersucht.

Zum Beweis betrachten wir ein schiefes Produkt $R \circ P$. Damit dies ein Ring ist, ist notwendig und hinreichend, daß die Addition (1) kommutativ, assoziativ und invertierbar, die Multiplikation (2) assoziativ ist, ferner die links- und rechtsseitige Distributivität gilt.

Die Kommutativitätsbedingung der Addition drückt sich durch (K) aus.

Die Assoziativitätsbedingung der Addition lautet nach (1)

$$(8) \qquad [\alpha, \beta] + [[a, b] + \alpha + \beta, \gamma] = [\alpha, [b, c] + \beta + \gamma] + [\beta, \gamma].$$

Es genügt zu zeigen, daß unter Berücksichtigung der Anfangsbedingungen (B) die Bedingung (8) mit den Bedingungen (A_1^+), (A_2^+) äquivalent ist. Wird in (8) $\alpha = o$ bzw. $b = 0$ eingesetzt, so entstehen nach (B) die mit (8) äqui-

valenten Relationen:

$$[[a, b]+\beta, \gamma]=[\beta, \gamma] \tag{9}$$

und (A_1^+). Die Bedingung (9) ist aber wegen (A_1^+) mit (A_2^+) äquivalent.

Da $(0, o)$ das Zeroelement von $R \circ P$ ist, genügt es die Existenz des additiven Inversen in $R \circ P$ nachzuweisen. Es gilt

$$(a, \alpha)=(a, o)+(0, \alpha)$$

wegen (1) und (B), ferner

$$(a, o)+(-a, -[a, -a])=(0, o), \qquad (0, \alpha)+(-[\alpha, -\alpha], \alpha)=(0, o).$$

Hieraus folgt für das additive Inverse

$$-(a, \alpha)=(-a-[\alpha, -\alpha], -[a, -a]-\alpha).$$

Die Bedingung der linksseitigen Distributivität lautet nach (1), (2)

$$\begin{aligned}(ab+ac+a[\beta, \gamma]+a^{[b, c]+\beta+\gamma}+{}^{\alpha}(b+c+[\beta, \gamma])+\{\alpha, [b, c]+\beta+\gamma\},\\ \{a, b+c+[\beta, \gamma]\}+\alpha^{b+c+[\beta, \gamma]}+{}^{\alpha}([b, c]+\beta+\gamma)+\alpha[b, c]+\beta+\gamma)=\\ =(ab+a^{\beta}+{}^{\alpha}b+\{\alpha, \beta\}, \{a, b\}+\alpha^{b}+{}^{\alpha}\beta+\alpha\beta)+\\ +(ac+a^{\gamma}+{}^{\alpha}c+\{\alpha, \gamma\}, \{a, c\}+\alpha^{c}+{}^{\alpha}\gamma+\alpha\gamma),\end{aligned}$$

d. h.

$$\begin{aligned}a[\beta, \gamma]+a^{[b, c]+\beta+\gamma}+{}^{\alpha}(b+c+[\beta, \gamma])+\{\alpha, [b, c]+\beta+\gamma\}=\\ =a^{\beta}+a^{\gamma}+{}^{\alpha}b+{}^{\alpha}c+\{\alpha, \beta\}+\{\alpha, \gamma\}+\\ +[\{a, b\}+\alpha^{b}+{}^{\alpha}\beta+\alpha\beta, \{a, c\}+\alpha^{c}+{}^{\alpha}\gamma+\alpha\gamma],\end{aligned} \tag{10}$$

und eine ähnliche Gleichung gilt für die duale Formel.

Die Bedingung für die rechtsseitige Distributivität entsteht aus (10) dadurch, daß man die Reihenfolge der Faktoren vertauscht und die Funktionen $\{\xi, \eta\}, x^{\xi}, {}^{\xi}x$ der Reihe nach durch $\{\eta, \xi\}, {}^{\xi}x, x^{\xi}$ ersetzt. Auf Grund dieser Tatsache, wenn eine Formel aus der linksseitigen Distributivität folgt, so liefert diese Ersetzung wieder eine gültige Formel, die genau die analoge Folgerung der rechtsseitigen Distributivität ist. Zum Zweck des leichteren Ausdrucks werden wir dieses Verfahren das *Symmetrisieren* des betreffenden Beweises nennen. Die dadurch entstehenden neuen Formeln werden die *symmetrisierten* der ursprünglichen Formeln genannt.

Im folgenden werden wir zu einer Formel stets auch die symmetrisierte und duale hinzunehmen.

Die Behauptung läßt sich dann so aussprechen, daß (10) mit (D_1) bis (D_5) äquivalent ist.

Für $\beta = o, c = 0$ ergibt (10) wegen der Invertierbarkeit der Addition die Bedingung (D_5). Ferner, wenn wir in (10)

$$\left.\begin{array}{l} a = 0, \beta = \gamma = o \\ b = c = 0, \alpha = o \\ a = b = c = 0 \\ \alpha = \beta = \gamma = o \end{array}\right\} \text{einsetzen, so entstehen} \left\{\begin{array}{l} (D_1), \\ (D_2), \\ (D_3), \\ (D_4). \end{array}\right.$$

Um die Umkehrung, d. h. daß (10) eine Folgerung der Bedingungen (D_1) bis (D_5) ist, zu beweisen, zeigen wir zuerst, daß aus (K), (A_1^+), (A_2^+) und (D_1) bis (D_5) noch die hier anschließend abzuleitenden Gleichungen folgen.

Aus (A_1^+) folgt

$$[\alpha_1 + \alpha_2, \beta_1 + \beta_2] + [\alpha_1, \alpha_2] + [\beta_1, \beta_2] = [\alpha_1 + \beta_1, \alpha_2 + \beta_2] + [\alpha_1, \beta_1] + [\alpha_2, \beta_2]. \tag{11}$$

Die Gleichungen

$$[\{a, b\}, {}^a\gamma] = [\alpha^b, \alpha\gamma] = 0 \tag{12}$$

sind einfache Folgerungen von (D_5), wenn man in (D_5) $\alpha = o$ bzw. $a = 0$ einsetzt. Wegen (11) und (12) ist (D_5) mit

$$[\{a, b\} + {}^{''}\gamma, \alpha^b + \alpha\gamma] = 0 \tag{13}$$

äquivalent.

Es gelten auch die folgenden:

$$[\alpha^b + \alpha\beta, \alpha^c + \alpha\gamma] = [\alpha[b, c], \alpha(\beta + \gamma)] + [\alpha\beta, \alpha\gamma] + [\alpha^b, \alpha^c], \tag{14}$$

$$[\{a, b\} + {}^a\beta, \{a, c\} + {}^a\gamma] = [{}^a[b, c], {}^a(\beta + \gamma)] + [\{a, b\}, \{a, c\}] + [{}^a\beta, {}^a\gamma]. \tag{15}$$

Die Gleichung (14) sieht man so ein. Wegen (11) und (12) ist

$$[\alpha^b + \alpha\beta, \alpha^c + \alpha\gamma] = [\alpha^b + \alpha^c, \alpha(\beta + \gamma)] + [\alpha\beta, \alpha\gamma] + [\alpha^b, \alpha^c].$$

Es genügt zu zeigen, daß

$$[\alpha^b + \alpha^c, \alpha(\beta + \gamma)] = [\alpha[b, c], \alpha(\beta + \gamma)].$$

Unter Berücksichtigung von (9) (d. h. (A_1^+), (A_2^+)), (D_2), (11) und (12) ergibt sich

$$[\alpha^b + \alpha^c, \alpha(\beta + \gamma)] = [\alpha^b + \alpha^c + [{}^a b, {}^a c], \alpha(\beta + \gamma)] = [\alpha[b, c] + \alpha^{b+c}, \alpha(\beta + \gamma)] =$$
$$= [\alpha(\beta + \gamma + [b, c]), \alpha^{b+c}] + [\alpha(\beta + \gamma), \alpha[b, c]] = [\alpha[b, c], \alpha(\beta + \gamma)],$$

was zu beweisen war.

Wenden wir (11) auf die linke Seite von (15) an, so gilt

$$[\{a, b\} + {}^{''}\beta, \{a, c\} + {}^{''}\gamma] = [{}^{''}\beta + {}^{''}\gamma, \{a, b\} + \{a, c\}] + [\{a, b\}, \{a, c\}] + [{}^a\beta, {}^a\gamma].$$

Also hat man nur noch

$$[{}^{''}\beta + {}^{''}\gamma, \{a, b\} + \{a, c\}] = [{}^{''}[b, c], {}^{''}(\beta + \gamma)] \tag{16}$$

einzusehen. Die linke Seite ist nach (9) (d. h. (A_1^+) und (A_2^+)), (D_1), (D_3) und (11)

$$\begin{aligned}[{}^{a}\beta+{}^{a}\gamma, \{a,b\}+\{a,c\}] &= [{}^{a}\beta+{}^{a}\gamma+[a^{\beta}, a^{\gamma}], \{a,b\}+\{a,c\}+[ab,ac]] = \\ &= [{}^{a}(\beta+\gamma)+\{a,[\beta,\gamma]\}, {}^{a}[b,c]+\{a,b+c\}] = \\ &= [{}^{a}(\beta+\gamma)+{}^{a}[b,c], \{a,[\beta,\gamma]\}+\{a,b+c\}]+[\{a,[\beta,\gamma]\}, \{a,b+c\}]+ \\ &\quad +[{}^{a}(\beta+\gamma), {}^{a}[b,c]].\end{aligned}$$

Der zweite Summand verschwindet hier wegen (D_4) und (A_2^+). Jetzt beweisen wir, daß auch das erste Glied verschwindet. Dieses ist von ähnlicher Form, wie die linke Seite von (16). Folglich ist

$$\begin{aligned}[{}^{a}(\beta+\gamma)+{}^{a}[b,c], \{a,[\beta,\gamma]\}+\{a,b+c\}] &= \\ = [{}^{a}(\beta+\gamma+[b,c])+{}^{a}[[\beta,\gamma],b+c], \{a,[\beta+\gamma,[b,c]\}+\{a,[\beta,\gamma]+b+c\}]+ \\ +[{}^{a}(\beta+\gamma+[b,c]), {}^{a}[[\beta,\gamma],b+c]].\end{aligned}$$

Das letzte Glied ist wegen (A_2^+) gleich 0, das erste kann man wegen (A_2^+) als

$$[{}^{a}(\beta+\gamma+[b,c]), \{a,[\beta,\gamma]+b+c\}]$$

schreiben. Da dieses nach (12) verschwindet, so haben wir (15) bewiesen.

Im folgenden benötigen wir die folgende Gleichung:

$$\begin{aligned}(17)\qquad [\{a,b\}+{}^{a}\beta+\alpha^{b}+\alpha\beta, \{a,c\}+{}^{a}\gamma+\alpha^{c}+\alpha\gamma] &= \\ = [\{a,b\}+{}^{a}\beta, \{a,c\}+{}^{a}\gamma]+[\alpha^{b}+\alpha\beta, \alpha^{c}+\alpha\gamma]&.\end{aligned}$$

Um diese zu beweisen, formen wir die linke Seite nach (12) und (11) um:

$$\begin{aligned}&[\{a,b\}+{}^{a}\beta, \{a,c\}+{}^{a}\gamma]+[\alpha^{b}+\alpha\beta, \alpha^{c}+\alpha\gamma]+ \\ &+[\{a,b\}+{}^{a}\beta+\{a,c\}+{}^{a}\gamma, \alpha^{b}+\alpha^{c}+\alpha(\beta+\gamma)].\end{aligned}$$

Der letzte Summand ist wegen (A_2^+) gleich

$$[\{a,b\}+\{a,c\}+[ab,ac]+{}^{a}\beta+{}^{a}\gamma+[a^{\beta}, a^{\gamma}], \alpha^{b}+\alpha^{c}+[{}^{a}b, {}^{a}c]+\alpha(\beta+\gamma)].$$

Hieraus folgt nach (D_3), (D_1) und (D_2)

$$\begin{aligned}[{}^{a}[b,c]+\{a,b+c\}+{}^{a}(\beta+\gamma)+\{a,[\beta,\gamma]\}, \alpha[b,c]+\alpha^{b+c}+\alpha(\beta+\gamma)] &= \\ = [{}^{a}([b,c]+\beta+\gamma)+\{a,[[b,c],\beta+\gamma]\}+ \\ +{}^{a}[b+c,[\beta,\gamma]]+\{a,b+c+[\beta,\gamma]\}, \alpha([b,c]+\beta+\gamma)+\alpha^{b+c}]&.\end{aligned}$$

Wenn man hier (A_2^+) berücksichtigt, folgt wegen (D_5) das Verschwinden dieses Gliedes.

Wir sind schon in der Lage die Bedingung (10) der (linksseitigen) Distributivität aus (K), (A_1^+), (A_2^+), (D_1)—(D_5) leicht zu beweisen. Mit wiederholter Anwendung von (D_1)—(D_4) bekommt man

$$\begin{aligned}(18)\qquad {}^{a}(b+c+[\beta,\gamma]) &= {}^{a}(b+c+[\beta,\gamma])+\{\alpha,[b+c,[\beta,\gamma]]\} = \\ = {}^{a}(b+c)+{}^{a}[\beta,\gamma]+[\alpha^{b+c}, \alpha^{[\beta,\gamma]}] &= {}^{a}b+{}^{a}c+[\alpha^{b}, \alpha^{c}]-\{\alpha,[b,c]\},\end{aligned}$$

ferner

$$
\begin{aligned}
a[\beta,\gamma]+a^{[b,c]+\beta+\gamma} &= a[\beta,\gamma]+a^{[b,c]+\beta+\gamma}+a[[b,c],\beta+\gamma]= \\
&= a[\beta,\gamma]+a^{[b,c]}+a^{\beta+\gamma}+[{}^{a}[b,c],{}^{a}(\beta+\gamma)]= \\
&= [\{a,b\},\{a,c\}]+a^{\beta}+a^{\gamma}+[{}^{a}\beta,{}^{a}\gamma]+[{}^{a}[b,c],{}^{a}(\beta+\gamma)],
\end{aligned} \tag{19}
$$

endlich

$$
\begin{aligned}
\{\alpha,[b,c]+\beta+\gamma\} &= \{\alpha,[b,c]+\beta+\gamma\}+{}^{\alpha}[[b,c],\beta+\gamma]= \\
&= \{\alpha,[b,c]\}+\{\alpha,\beta+\gamma\}+[\alpha[b,c],\alpha(\beta+\gamma)]= \\
&= \{\alpha,[b,c]\}+\{\alpha,\beta\}+\{\alpha,\gamma\}+\{\alpha\beta,\alpha\gamma\}-{}^{\alpha}[\beta,\gamma]+[\alpha[b,c],\alpha(\beta+\gamma)].
\end{aligned}
$$

Die Summe der linken Seiten von (18), (19), (20) ist eben die linke Seite von (10). Da die Formeln (14), (15) und (17) nach obigem Folgerungen der Bedingungen (D_1) bis (D_5) (und (K), (A_1^+), (A_2^+)) sind und die Summe der rechten Seiten von (18)—(20) nach (14), (15) und (17) der rechten Seite von (10) gleich ist, folgt die Äquivalenz der Bedingungen (10) und (D_1)—(D_5).

Es genügt also noch zu zeigen, daß unter Berücksichtigung von (B) die Assoziativität der Multiplikation mit den Bedingungen (A_1)—(A_6) äquivalent ist. Da nach (1) die Zerlegung $(a,\alpha)=(a,o)+(0,\alpha)$ gilt, so genügt es wegen der Distributivität, daß man die Bedingungen der Assoziativität der Multiplikation für die Elemente von der Form (a,o), $(0,\alpha)$ aufstellt. Es kommen die acht Dreierprodukte

(21)	$(a,o)(b,o)(c,o)$,	$(0,\alpha)(0,\beta)(0,\gamma)$,
(22)	$(a,o)(b,o)(0,\gamma)$,	$(0,\alpha)(b,o)(c,o)$,
(23)	$(a,o)(0,\beta)(0,\gamma)$,	$(0,\alpha)(0,\beta)(c,o)$,
(24)	$(a,o)(0,\beta)(c,o)$,	$(0,\alpha)(b,o)(0,\gamma)$

in Betracht. Für die Produkte (21_1) und (21_2) sind die Assoziativitätsbedingungen nach (2) mit (A_1) bzw. (A_2) äquivalent. Aus (22) und (23) ergeben sich die Bedingungen (A_5) und (A_6). Endlich sind für (24_1), (24_2) die Assoziativitätsbedingungen eben (A_3) und (A_4), womit Satz 1 bewiesen ist.

§ 3. Spezialfälle.

A. EVERETT [2] hat nach SCHREIER die folgende Definition eingeführt: Man nenne einen Ring $\mathfrak{R}$ eine Erweiterung von P mit R, wenn $\mathfrak{R}$ ein Ideal P' hat, wofür $P' \approx P$, $\mathfrak{R}/P' \approx R$ gilt. Man darf natürlich $P' = P$ setzen, wie das üblich ist. Die angegebene Form der Definition ist aber für unsere Zwecke bequemer.

Der folgende Satz stimmt im wesentlichen mit dem Hauptsatz der Erweiterungstheorie von EVERETT [2] überein (siehe auch RÉDEI [6]):

Ein schiefes Produkt $\mathfrak{R} = R \in \mathsf{P}$ *der Ringe* R, P *ist dann und nur dann ein Ring, wenn*

$$(E_1) \qquad [a, b] = [b, a],$$

$$(E_2) \qquad [a, b] + [a+b, c] = [a, b+c] + [b, c],$$

$$(E_3) \qquad {}^{a}\{b, c\} + \{a, bc\} = \{a, b\}^{c} + \{ab, c\},$$

$$(E_4) \qquad \alpha({}^{b}\gamma) = (\alpha^{b})\gamma,$$

$$(E_5) \qquad {}^{a}(\beta^{c}) = ({}^{a}\beta)^{c},$$

$$(E_6) \qquad \alpha(\beta^{c}) = (\alpha\beta)^{c}, \qquad ({}^{a}\beta)\gamma = {}^{a}(\beta\gamma),$$

$$(E_7) \qquad (\alpha^{b})^{c} = \alpha^{bc} + \alpha\{b, c\}, \qquad {}^{a}({}^{b}\gamma) = {}^{ab}\gamma + \{a, b\}\gamma,$$

$$(E_8) \qquad {}^{a}(\beta+\gamma) = {}^{a}\beta + {}^{a}\gamma, \qquad (\alpha+\beta)^{c} = \alpha^{c} + \beta^{c},$$

$$(E_9) \qquad \alpha^{b+c} + \alpha[b, c] = \alpha^{b} + \alpha^{c}, \qquad {}^{a+b}\gamma + [a, b]\gamma = {}^{a}\gamma + {}^{b}\gamma,$$

$$(E_{10}) \qquad \begin{aligned} {}^{a}[b, c] + \{a, b+c\} &= [ab, ac] + \{a, b\} + \{a, c\}, \\ [a, b]^{c} + \{a+b, c\} &= \{ac, bc\} + \{a, c\} + \{b, c\}. \end{aligned}$$

gelten. Diese Ringe sind bis auf Isomorphie die sämtlichen Everettschen Erweiterungen von P *mit* R*, und zwar bilden dann die Elemente* $(0, \alpha)$ *ein Ideal* P' *von* $\mathfrak{R}$*, wofür*

$$\mathfrak{R}/\mathsf{P}' \approx R((a, o) + \mathsf{P}' \to a), \quad \mathsf{P}' \approx \mathsf{P}((0, \alpha) \to \alpha)$$

gilt.

Die erste Behauptung dieses Satzes ist bloß der Spezialfall $[\alpha, \beta] = \{\alpha, \beta\} = a^{\beta} = {}^{\alpha}b = 0$ vom Satz 1. Die Beweise der übrigen Behauptungen dieses Satzes kann man in [2], [6] finden.

Für Ergänzungen der Everettschen Erweiterungstheorie verweisen wir auf [6], [10],[3]) [11].

B. Wir wollen jetzt die Ringe $R \circ \mathsf{P}$ aus (5) bestimmen. Wir haben schon in der Einleitung bemerkt, daß diese Ringe mit den Szépschen Erweiterungen identisch sind. Bezeichnen $\mathfrak{R}$ und $\mathfrak{S}_1, \mathfrak{S}_2$ $(\mathfrak{S}_1 \cap \mathfrak{S}_2 = 0)$ einen belie-

---

[3]) Wir berichtigen einen Fehler in der zitierten Arbeit, und zwar sind dort auf Seite 180 die Wörter „splitting" in den Zeilen 1, 10, 18 zu streichen und die Zeilen 13—16 durch die folgenden zu ersetzen:

$$(\bar{a}, \alpha) + (\bar{b}, \beta) = (\overline{a+b}, [\bar{a}, \bar{b}] + \alpha + \beta),$$

$$(\bar{a}, \alpha)(\bar{b}, \beta) = (\overline{a+b}, \{\bar{a}, \bar{b}\} + \alpha\bar{b} + \bar{a}\beta + \alpha\beta),$$

where $[\bar{a}, \bar{b}] = \left[\frac{a+b}{m}\right]\mu$, $\{\bar{a}, \bar{b}\} = \left[\frac{ab}{m}\right]\mu$ if $m > 0$, denoting by μ the element of P for which $m\xi = \mu\xi = \xi\mu$, and $[\bar{a}, \bar{b}] = \{\bar{a}, \bar{b}\} = o$ if $m = 0$, finally $\bar{x}\xi = \xi\bar{x} = x\xi$. ($x$ denotes the least non-negative representative of the residue class $\bar{x}$.)

bigen Ring bzw. zwei echte Unterringe von $\mathfrak{R}$, gilt ferner[4])

$$\mathfrak{R}^+ = \mathfrak{S}_1^+ + \mathfrak{S}_2^+,$$

wo $+$ das Zeichen der direkten Summe ist, so wird $\mathfrak{R}$ in Bezug auf die Addition *zerlegbar* genannt.

Als Umkehrung tritt das dem Everettschen ähnliche Szépsche Erweiterungsproblem auf, aus gegebenen Ringen R, P alle Ringe $\mathfrak{R}$ mit

$$\mathfrak{R}^+ = \mathfrak{S}_1^+ + \mathfrak{S}_2^+, \quad \mathfrak{S}_1 \approx R, \ \mathfrak{S}_2 \approx \mathsf{P} \quad (\mathfrak{S}_1 \cap \mathfrak{S}_2 = 0)$$

zu bestimmen, wo $\mathfrak{S}_1$ und $\mathfrak{S}_2$ Unterringe von $\mathfrak{R}$ sind.

Es gilt der von SZÉP herrührende Satz:

Das schiefe Produkt $R \circ \mathsf{P}$ der Ringe R und P ist dann und nur dann ein Ring, wenn

$$(S_1) \qquad a({}^{\beta}c) + a^{({}^{\beta}c)} = (a^{\beta})c + {}^{({}^{\alpha}\beta)}c,$$

$$(S_2) \qquad {}^{\alpha}(b^{\gamma}) = ({}^{\alpha}b)^{\gamma},$$

$$(S_3) \qquad a(b^{\gamma}) + a^{{}^{b}\gamma} = (ab)^{\gamma}, \quad ({}^{\alpha}b)c + {}^{\alpha^{b}}c = {}^{\alpha}(bc),$$

$$(S_4) \qquad (a^{\beta})^{\gamma} = a^{\beta\gamma}, \quad {}^{\alpha}({}^{\beta}c) = {}^{\alpha\beta}c,$$

$$(S_5) \qquad {}^{\alpha}(b+c) = {}^{\alpha}b + {}^{\alpha}c, \quad (a+b)^{\gamma} = a^{\gamma} + b^{\gamma},$$

$$(S_6) \qquad a^{\beta+\gamma} = a^{\beta} + a^{\gamma}, \quad {}^{\alpha+\beta}c = {}^{\alpha}c + {}^{\beta}c$$

und die duale Gleichungen gelten. Diese Ringe sind bis auf Isomorphie die sämtlichen Szépschen Erweiterungen von R und P.

Die Elemente (a, o) bzw. $(0, \alpha)$ bilden je einen Unterring (R, o), $(0, \mathsf{P})$, — denn

$$(a, o) + (b, o) = (a+b, o), \quad (0, \alpha) + (0, \beta) = (0, \alpha+\beta),$$
$$(a, o)(b, o) = (ab, o), \quad (0, \alpha)(0, \beta) = (0, \alpha\beta)$$

gelten, woraus $(R, o) \approx R$ und $(0, \mathsf{P}) \approx \mathsf{P}$, ferner

$$(R \circ \mathsf{P})^+ = (R, o)^+ + (0, \mathsf{P})^+$$

folgen.

Die erste Behauptung des Satzes ergibt sich sofort aus Satz 1 als der Spezialfall $[\alpha, \beta] = \{\alpha, \beta\} = 0$, $[a, b] = \{a, b\} = o$. Für die übrigen Behauptungen und anderen Ergänzungen der Szépschen Erweiterungen verweisen wir auf seine Arbeit [12].

C. Wir wollen uns mit dem sehr interessanten schiefen Produkt $R * \mathsf{P}$ beschäftigen, das 5-fach ausgeartet ist. Es gilt als Spezialfall von Satz 1 der folgende Satz

---

[4]) T^+ bezeichnet die additive Gruppe des Ringes T.

Das schiefe Produkt $R*\mathsf{P}$ ist dann und nur dann ein Ring, wenn

(I) $$\alpha({}^{b}\gamma) = ({}^{b}\alpha)\gamma,$$

(II) $${}^{a}(\beta^{c}) = ({}^{a}\beta)^{c},$$

(III) $$\alpha(\beta^{c}) = (\alpha\beta)^{c}, \qquad ({}^{a}\beta)\gamma = {}^{a}(\beta\gamma),$$

(IV) $$(\alpha^{b})^{c} = \alpha^{bc}, \qquad {}^{a}({}^{b}\gamma) = {}^{ab}\gamma,$$

(V) $${}^{a}(\beta+\gamma) = {}^{a}\beta + {}^{a}\gamma, \qquad (\alpha+\beta)^{c} = \alpha^{c} + \beta^{c},$$

(VI) $$\alpha^{b+c} = \alpha^{b} + \alpha^{c}, \qquad {}^{a+b}\gamma = {}^{a}\gamma + {}^{b}\gamma,$$

(VII) $$\alpha^{\{\beta,\gamma\}} = {}^{\{\alpha,\beta\}}\gamma,$$

(VIII) $$\{\alpha, \beta\gamma\{ = \{\alpha\beta, \gamma\},$$

(IX) $$\{\alpha, {}^{b}\gamma\} = \{\alpha^{b}, \gamma\},$$

(X) $$\{{}^{a}\beta, \gamma\} = a\{\beta, \gamma\}, \qquad \{\alpha, \beta^{c}\} = \{\alpha, \beta\}c,$$

(XI) $$\{\alpha, \beta+\gamma\} = \{\alpha, \beta\} + \{\alpha, \gamma\}, \quad \{\alpha+\beta, \gamma\} = \{\alpha, \gamma\} + \{\beta, \gamma\}$$

gelten.

Wir kommen jetzt zu einer Anwendung des schiefen Produktes $R*\mathsf{P}$.

Hier bezeichnen R und R_0 einen beliebigen Ring mit Einselement, bzw. einen Zeroring, dessen additive Gruppe zu der additiven Gruppe von R isomorph ist. Die Elemente von R und R_0 werden mit $0, a, b, \ldots$ bzw. $0_0, a_0, b_0, \ldots$ bezeichnet, so daß die Abbildung $a \to a_0$ einen Isomorphismus von R^+ auf R_0^+ liefert. Wir betrachten das schiefe Produkt $R*R_0$ der Ringe R und R_0, wobei die vorkommenden Funktionen durch

$$\{a_0, b_0\} = -ab, \quad {}^{a}b_0 = (ab)_0, \quad a_0^{b} = (ab)_0$$

definiert werden.

Nach den obigen ist $R*R_0$ ein Ring, die mit dem *komplexen Ring über* R isomorph ist. Wir betrachten nämlich den komplexen Ring R über R. Die Elemente von R — wie es üblich ist — kann man in der Form $a+bi$ angeben. Dann liefert die Abbildung

$$a + bi \to (a, b_0)$$

von R auf $R*R_0$ einen passenden Isomorphismus.

Wenn R insbesondere der Körper $\mathfrak{R}$ der reellen Zahlen ist, so ist $\mathfrak{R}*\mathfrak{R}_0$ isomorph mit dem Körper K der komplexen Zahlen.

Betrachten wir jetzt das schiefe Produkt $\mathsf{R}*\mathsf{R}_0$, wobei R den komplexen Ring über einem Ring R mit Einselement und R_0 einen Zeroring mit $\mathsf{R}_0^+ \approx \mathsf{R}^+$ bezeichnet. Es seien $0, \alpha, \beta, \ldots,$ und $0_0, \alpha_0, \beta_0, \ldots$ die Elemente von R bzw. R_0 und es gelte der Isomorphismus $\mathsf{R}^+ \approx \mathsf{R}_0^+ (\alpha \to \alpha_0)$. Die jetzt vorkommenden Funktionen werden durch

$$\{\alpha_0, \beta_0\} = -\alpha\bar{\beta}, \quad {}^{\alpha}\beta_0 = (\alpha\beta)_0, \quad \alpha_0^{\beta} = (\alpha\bar{\beta})_0$$

definiert, wobei $\bar{\xi}$ das Konjugierte von ξ bezeichnet. Nach Satz 4 ist $R * R_0$ ein Ring, der mit dem *Quaternionenring* Q (über R) isomorph ist.

Die Elemente des Quaternionenringes Q über R kann man bekanntlich in der Form $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ annehmen. Ein Isomorphismus von auf $R * R_0$ ist dann durch

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \to (\alpha, \beta_0)$$

angegeben.

Wird R mit dem Körper K der komplexen Zahlen identifiziert, so ergibt sich, daß $K * K_0$ mit dem Quaternionenkörper über $\mathfrak{R}$ isomorph ist.

D. Man gewinnt durch die Spezialisierung $[\alpha, \beta] = \{\alpha, \beta\} = \alpha^\beta = {}^\alpha b = 0$, $[a, b] = \{a, b\} = o$ die folgende Behauptung:

Das schiefe Produkt $R \bullet P$ der Ringe R und P aus (7) *ist dann und nur dann ein Ring, wenn die Gleichungen* (I) *bis* (VI) *aus dem Spezialfall* **C** *gelten.*

Diese Ringkonstruktion, die als die faktorenfreie Everettsche Erweiterung von P mit R bekannt ist, ist ein Spezialfall sowohl der Everettschen als auch der Szépschen Erweiterungen.

Diese Konstruktion geht im Fall $\alpha^b = {}^b\alpha$ auf DORROH [1] zurück. Er hat mit dieser Hilfe bewiesen, daß jeder Ring P eine Erweiterung mit Einselement hat. In seinem Fall ist $R = \mathfrak{Z}$ der Ring der ganzen rationalen Zahlen, ferner sind jetzt α^b, ${}^b\alpha$ durch $\alpha^b = {}^b\alpha = b\alpha$ definiert, weshalb die obigen Bedingungen (I) bis (VI) trivialerweise erfüllt sind.

§ 4. Das Isomorphieproblem des schiefen Produktes $R \circ P$.

Endlich wollen wir uns noch mit dem Isomorphieproblem des schiefen Produktes $R \circ P$ beschäftigen. Dieses Problem besteht darin, daß man bei gegebenen Ringen R, P die sämtlichen isomorphen schiefen Produkte $R \circ P$ bestimmt. Es genügt vollkommen, daß man einen Ring $R \circ P$ gleich in der Form von Satz 1 annimmt, was wir im folgenden stets tun wollen. Ausdrücklich gesagt bedeutet das, daß man einen Ring $R \circ P$ durch (1), (2) und (B) definiert. Das hat den großen Vorteil, daß bei festen R und P die sämtlichen schiefen Produkte $R \circ P$ aus denselben Elementen (a, α) bestehen. Die vollständige Lösung des Isomorphieproblems ist sehr schwer. Das weiteste, was wir in dieser Richtung sagen können, ist im folgenden Satz enthalten.

Satz 2. *Man nehme ein schiefes Produkt $R \circ P$ aus Satz 1. Mit dem zugehörigen Funktionenachter* (3) *zusammen genügt auch jeder Funktionen-*

achter

$$(25)\qquad \begin{aligned} &A^{-1}[A\alpha, A\beta],\ A^{-1}\{A\alpha, A\beta\},\ A^{-1}((Aa)^{L\beta}),\ A^{-1}({}^{A\alpha}(Ab)),\\ &A^{-1}[Aa, Ab],\ A^{-1}\{Aa, Ab\},\ A^{-1}((A\alpha)^{Ab}),\ A^{-1}({}^{Aa}(A\beta)),\end{aligned}$$

den Bedingungen (B), (K) *bis* (D_5), *wobei* $a \to Aa$ *und* $\alpha \to A\alpha$ *einem Automorphismus von* R *bzw.* P *bezeichnet. Werden in* (1), (2) *die acht Funktionen durch* (25) *ersetzt, so entsteht wieder ein schiefes Produkt und es gilt zwischen ihnen der Isomorphismus*

$$(26)\qquad (a, \alpha) \to (Aa, A\alpha).$$

Zum Beweis nehmen wir vor allem in acht, daß der Funktionenachter (25) offenbar den Bedingungen (B) genügt. Nun betrachten wir die Permutation $(a, \alpha) \to \Pi^{-1}(a, \alpha) = (Aa, A\alpha)$ der Elemente von $R \circ P$. Nach dem bekannten allgemeinen Prinzip (s. RÉDEI [4] § 3) liefert der Übergang zu den neuen Verknüpfungen

$$(a, \alpha) \oplus (b, \beta) = \Pi(\Pi^{-1}(a, \alpha) + \Pi^{-1}(b, \beta)),$$
$$(a, \alpha) \odot (b, \beta) = \Pi(\Pi^{-1}(a, \alpha)\,\Pi^{-1}(b, \beta))$$

eine zu $R \circ P$ isomorphe Struktur, und zwar gilt dabei der Isomorphismus (26). Ferner berechnen sich die rechten Seiten der vorigen Gleichungen zu

$$\Pi((Aa, A\alpha) + (Ab, A\beta)) = \Pi(Aa + Ab + [A\alpha, A\beta], [Aa, Ab] + A\alpha + A\beta) =$$
$$= (a + b + A^{-1}[A\alpha, A\beta], A^{-1}[Aa, Ab] + \alpha + \beta),$$

$$\Pi((Aa, A\alpha)(Ab, A\beta)) = \Pi(AaAb + (Aa)^{A\beta} +$$
$$+ {}^{A\alpha}(Ab) + \{A\alpha, A\beta\}, \{Aa, Ab\} + (A\alpha)^{Ab} + {}^{Aa}(A\beta) + A\alpha A\beta) =$$
$$= (ab + A^{-1}((Aa)^{A\beta}) + A^{-1}({}^{A\alpha}(Ab)) + A^{-1}\{A\alpha, A\beta\}, A^{-1}\{Aa, Ab\} +$$
$$+ A^{-1}((A\alpha)^{Ab}) + A^{-1}({}^{Aa}(A\beta)) + \alpha\beta).$$

Der Vergleich mit (1) und (2) beweist (25), ferner folgt aus Satz 1 mit Notwendigkeit, daß für (25) auch (K)—(D_5) gelten. Somit haben wir Satz 2 bewiesen.

Insbesondere für das Isomorphieproblem des schiefen Produktes $R \in P$ verweisen wir auf RÉDEI [6].

Literaturverzeichnis.

[1] J. L. Dorroh, Concerning adjunctions to algebras, *Bulletin of the American Math. Society*, **38** (1932), 85—88.

[2] C. J. Everett, An extension theory for rings, *American Journal of Math.*, **64** (1942), 363—370.

[3] R. Kochendörffer, Zur Theorie der Rédeischen schiefen Produkte, *Journal für die reine und angewandte Math.*, **192** (1953), 96—101.

[4] L. Rédei, Die Anwendung des schiefen Produktes in der Gruppentheorie, *Journal für die reine und angewandte Math.*, **188** (1950), 201—227.

[5] L. Rédei, Über gewisse Ringkonstruktionen durch schiefes Produkt, *Acta Math. Acad. Sci. Hung.*, **2** (1951), 185—188.

[6] L. Rédei, Die Verallgemeinerung der Schreierschen Erweiterungstheorie, *Acta Sci. Math.*, **14** (1952), 252—273.

[7] L. Rédei und A. Stöhr, Über ein spezielles schiefes Produkt in der Gruppentheorie, *Acta Sci. Math.*, **15** (1953—54), 7—11.

[8] F. Rühs, Über ein spezielles Rédeisches schiefes Produkt in der Gruppentheorie, *Acta Sci. Math.*, **16** (1955), 160—164.

[9] G. Szász, Rédeische schiefe Produkte von Halbverbänden, *Acta Math. Acad. Sci. Hung.*, **7** (1957), 441—461.

[10] J. Szendrei, On Schreier extension of rings without zerodivisors, *Publicationes Math. Debrecen*, **2** (1952), 276—280.

[11] J. Szendrei, On rings admitting only direct extensions, *Publicationes Math. Debrecen*, **3** (1953), 180—182.

[12] J. Szép, Über eine neue Erweiterung von Ringen. I, *Acta Sci. Math.*, **19** (1958), 51—62.

(Eingegangen am 17. Oktober 1957.)

On complemented lattices.

By G. SZÁSZ in Szeged.

1. Introduction. In a recent paper the author has proved the following theorem ([5], Theorem 2) which may be considered as a converse of a well-known theorem of VON NEUMANN in the theory of complemented modular lattices:[1])

Theorem 1. *Let L be any relatively complemented lattice with greatest and least elements i, o, respectively, and let a, b, r be any elements of L such that $a \leqq r \leqq b$ holds. Let further s be any relative complement of r in $[a, b]$. If t is any solution of the equation system*

$$(1) \qquad \begin{cases} r \cap t = o, \; r \cup t = i, \\ (a \cup t) \cap b = s, \; a \cup (t \cap b) = s, \end{cases}$$

then there exists a relative complement y of a in $[o, s]$ and a relative complement z of b in $[s, i]$ such that t is a relative complement of s in $[y, z]$. Conversely, if y is any relative complement of a in $[o, s]$ and z is any relative complement of b in $[s, i]$, then any relative complement t of s in $[y, z]$ is a solution of (1).

It will be useful to complete the assertion of this theorem by the obvious

Remark. Let L, a, b be as in Theorem 1 and let r_1, r_2 be two distinct elements of $[a, b]$ which have a common relative complement s in $[a, b]$. Then, as one sees easily from Theorem 1, the two equation systems which may be obtained from (1) by substituting $r = r_1$ and $r = r_2$, respectively, have the same solutions; in particular, r_1 and r_2 have at least one common complement t.

The aim of this paper is to develop some applications of Theorem 1.

In section 2, firstly we give a condition which is necessary and sufficient for a relatively complemented lattice with greatest and least elements to

[1]) For this theorem see, e. g., [5], p. 48. — For the notations and the concepts used but not explained here, see [1].

be modular (Theorem 2). This condition is of similar kind as the condition which has been given by DILWORTH (in [2]) concerning the modularity of complemented lattices satisfying both chain conditions. Applying Theorem 2 and a generalization of the theorem of DILWORTH due to MCLAUGHLIN, we get another modularity condition for certain classes of complemented lattices (Theorem 3).

Section 3 is concerned with some contributions about the lattices with unique complements. Firstly we give a simple proof for the known theorem ([1], p. 171, ex. 2; in this paper Theorem 4) that any modular lattice with unique complements is a Boolean algebra. Afterwards, from Theorem 2 and 4, we derive the result that also any relatively complemented lattice with unique complements is distributive.

2. Modularity conditions. It is a remarkable theorem of DEDEKIND (see e. g. [1], p. 66) that a lattice L is modular if and only if no sublattice of L is isomorphic to the five-element lattice of Fig. 1. For complemented lattices satisfying the chain conditions, this theorem was sharpened by DILWORTH ([2], p. 21) in the following manner:

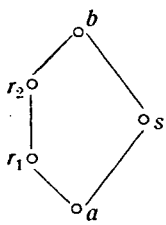

Fig. 1.

Let L be any complemented lattice which satisfies both the ascending chain condition and the descending one. Then L is modular if and only if no sublattice of L, including the greatest and the least elements of L, is isomorphic to the lattice of Fig. 1.

MCLAUGHLIN [4] has recently shown that the assertion of the DILWORTH theorem holds, more generally, for all atomic[2]) lattices. Now we show that it holds also for relatively complemented lattices with greatest and least elements.

For sake of brevity, we introduce the following definition: a sublattice S of a lattice with greatest element i and with least element o will be called *of Dilworth type* if $S \ni i, o$ and S isomorphic to the lattice of Fig. 1. Then we may formulate our theorem as follows:

Theorem 2. *Let L be any relatively complemented lattice with greatest and least elements. Then L is modular if and only if it contains no sublattice of Dilworth type.*

Proof. By the above-mentioned theorem of DEDEKIND, the condition is necessary. We show that it is also sufficient.

Let L be any relatively complemented lattice with greatest and least elements i, o, respectively. If L is non-modular, then — again by the theorem

[2]) A lattice L with least element o is called atomic if to each element $x(\neq o)$ of L there exists at least one element $p(\leqq x)$ which covers o.

of DEDEKIND — it contains a sublattice isomorphic to the lattice of Fig. 1. In other words, there exist elements a, b, r_1, r_2, s in L such that r_1 and r_2 have a common relative complement s in $[a, b]$. Hence, by Remark after Theorem 1, r_1 and r_2 have a common complement t. It follows that the set of elements o, r_1, r_2, t, i forms a sublattice of Dilworth type. This completes the proof of Theorem 2.

Before stating our second modularity condition announced in the introduction, we prove the following preliminary

Lemma. *Let L be any modular lattice with greatest and least elements i, o, respectively. If any elements a, b, c of L satisfy the equations*

$$a \cup c = i, \tag{2}$$

$$b \cap c = o, \tag{3}$$

then either $a \geqq b$ or a and b are incomparable.

Proof. Let V be any lattice with o and i in which the equations (2), (3) are satisfied by certain elements a, b, c such that $a < b$. It follows immediately that $a \cap c \leqq b \cap c = o$ and $b \cup c \geqq a \cup i = i$, whence

$$a \cap c = o, \quad b \cup c = i. \tag{4}$$

Next we show that for these elements also the inequalities

$$o < c < i, \quad o < a < b < i \tag{5}$$

hold. Indeed, $a < b$ holds by our assumption; further by (2) $o = c$ would imply $a = i$, by (3) $c = i$ would imply $b = o$, and both are impossible because of $a < b$; finally, by (2) $o = a$ would imply $c = i$ and by (3) $b = i$ would imply $c = o$ which we have just now shown to be impossible. It follows, by (2)—(5), that the elements o, a, b, c, i form a sublattice of V isomorphic to the lattice of Fig. 1. Hence, by the theorem of Dedekind, V is not modular.

Now we prove

Theorem 3. *Let L be any complemented lattice which has at least one of the following properties:* (i) *L is relatively complemented;* (ii) *L is atomic. Then L is modular if and only if for all elements a, b, c of L the equations* (2), (3) *and the equation $a \cap c = o$ imply that either $a \geqq b$ or a and b are incomparable.*[3])

Proof. The necessity of this condition is an obvious consequence of the Lemma. To prove its sufficiency, consider any complemented lattice L

[3]) This modularity condition is analogous te the following distributivity condition which is (implicitely) contained in the paper [3]: A complemented lattice L is distributive if the equations (2), (3) and the equation $a \cap c = o$ imply $a \geqq b$.

with the property (i) or (ii). If L is non-modular, then by our Theorem 2 or by the above-cited theorem of McLAUGHLIN, respectively, L contains a sublattice of Dilworth type; that is, there exist elements a, b, c in L such that $a < b$ and c is a common complement of a and b. This means that, in particular, (2), (3) and $a \cap c = o$ hold for a, b, c $(a < b)$. Hence we conclude that if L is non-modular, then also the condition of the theorem is not satisfied. This proves the sufficiency of the condition.

We remind the reader that the assumptions (i) resp. (ii) have been used only (in the proof of the sufficiency, namely) to infer the existence of a sublattice of Dilworth type. Accordingly, they may by replaced by any assumption (iii) which assures that if a complemented non-modular lattice satisfies (iii), then it contains a sublattice of Dilworth type.

3. Theorems on lattices with unique complements. First we give a new proof for the known

Theorem 4. *Any modular lattice with unique complements is a Boolean algebra.*

Proof. By a well-known theorem ([1], p. 134., Corollary 1 of Theorem 2) it is enough to show that, in every interval of a lattice having the properties prescribed in Theorem 4, also the relative complements are uniquely determined. For this purpose let a, b, r be any elements of a complemented modular lattice L such that $a \leqq r \leqq b$. By NEUMANN's Theorem, L is relatively complemented; therefore, Theorem 1 may be applied for L. It follows (from the second part of Theorem 1) that to each relative complement s of r there exists (at least) one complement t of r such that $s = a \cup (t \cap b)$. Hence, if L has also the property of being a lattice with unique complements, then r has (a unique complement t and, consequently) a unique relative complement s in $[a, b]$. Thus our theorem is proved.

Finally, as a consequence of Theorems 2 and 4, we get

Theorem 5. *A lattice with unique complements is relatively complemented if and only if it is distributive.*

Proof. Since any distributive (moreover, by NEUMANN's Theorem, any modular) complemented lattice is relatively complemented, the "if" part of the theorem is obvious.

Conversely, let L be any lattice with unique complements. If L is non-distributive, then by Theorem 4, it is even non-modular. But it is an obvious corollary of Theorem 2 that *non-modular lattices with unique complements are not relatively complemented.* Combining these two facts, we obtain the "only if" part of Theorem 5.

References.

[1] G. Birkhoff, *Lattice theory* (Amer. Math. Soc. Coll. Publ., vol. **25**), revised edition (New York, 1948).
[2] R. P. Dilworth, On complemented lattices, *Tôhoku Math. Journal*, **47** (1940), 18—23.
[3] E. V. Huntington, Sets of independent postulates for the algebra of logic, *Transactions Amer. Math. Soc.*, **5** (1904), 288—309.
[4] J. E. McLaughlin, Atomic lattices with unique comparable complements, *Proceedings Amer. Math. Soc.*, **7** (1956), 864—866.
[5] G. Szász, On relatively complemented lattices, *Acta Sci. Math.*, **18** (1957), 48—51.

(Received November 1, 1957.)

On ideal theory for lattices.

By G. GRÄTZER and E. T. SCHMIDT in Budapest.

1. Introduction.

The notion of lattice ideals plays an important role in lattice-theoretical researches. Recently J. HASHIMOTO [5] developed a theory of lattice ideals making effort to evolve this algebraic theory like that of rings. The fundamental tools of HASHIMOTO's paper are various topologies of lattices. Consequently, his purely lattice-theoretical assertions too are mostly proved with the apparatus of topology, so these proofs are not quite short and it is not easy to follow them.

The aim of the present paper is to prove in purely lattice-theoretical ways all purely lattice-theoretical theorems of [5]. These proofs are generally more concise than the original ones, further they offer more generalizations. In this paper we shall not deal with these generalizations. Related to these questions we refer to the papers [2], [3], [4].

In building up our paper we adhered strictly to the structure of HASHIMOTO's paper; the titles of the parts beginning from 3 — as well as the greatest part of the terminology — are identical with that of [5].

We should mention at last that all of the theorems, not containing explicitly the existence of prime ideals may be proved also without the Axiom of Choice (we hint here in the first line to the results in connexion with problems 72 and 73 of G. BIRKHOFF [1]). As for these proofs we refer to our above cited papers [2] and [3].

2. Some lemmas.

Before turning to HASHIMOTO's theorems we mention some lemmas in advance.

Lemma 1 (STONE's Theorem). *Let L be a distributive lattice and let I and D be any ideal resp. dual ideal of L such that I and D are disjoint.*

Among the ideals which are disjoint to D and contain I every maximal one is prime.[1])

The proof of this lemma runs along the same lines as the proof of the original assertion of STONE (see e. g. [1], p. 160).

Lemma II. *Let L be a distributive lattice. If the meet and the join of the ideals I and J are principal ideals, then I and J are principal ideals too.*

Proof. Let $I \cup J = (a]$ and $I \cap J = (b]$. It follows from the distributivity of L ([1], pp. 140—141) that for some $x, y \in I$ and $u, z \in J$, $x \cup z = a$ and $y \cap u = b$. It is easy to check that $(x \cup y) \cup (z \cup u) = a$ and $(x \cup y) \cap (z \cup u) = b$. We assert $I = (x \cup y]$ and $J = (z \cup u]$. If we had e. g. $I \neq (x \cup y]$, then there would exist in I an element w such that $x \cup y < w$. But then $w \cup (z \cup u) = a$ and $w \cap (z \cup u) = b$, that is, $z \cup u$ has two relative complements in the interval $[b, a]$, namely $x \cup y$ and w. It is well known that in a distributive lattice any element cannot have in every interval more than one relative complement, which contradicts the fact proved above and completes the proof of this lemma.

Lemma III. *Let L' be any homomorphic image of the lattice L and P' a prime ideal of L'. The complete inverse image of P' in L is a prime ideal.*

Proof. Let P be the complete inverse image of P'; evidently, P is an ideal. We prove that P is prime. Let us suppose that $x, y \notin P$, yet $x \cap y \in P$. Then, if we denote by x' and y' the homomorphic image of x and y, respectively, we get that x' and y' are not in P', for P is the complete inverse image of P'. Furthermore, $x' \cap y' = (x \cap y)' \in P'$, contradicting the assumption that P' is a prime ideal. Thus the proof is completed.

3. Possibility of factorization.

By a *representation* of a lattice L we mean here a homomorphism of L onto a distributive lattice. (This definition is not the same as, but is equivalent to, that of [5].)

Theorem I (Theorem 2.1 of [5]). *The following assertions concerning an ideal I of a lattice L are equivalent:*

---

[1]) This is a somewhat generalized form of STONE's Theorem, namely STONE restricts himself to the case when the dual ideal D is principal. The above form of the theorem has the advantage that every prime ideal P may be constructed in such a way (with $I = P$ and $D = L - P$), while originally only the completely meet-irreducible prime ideals could be constructed (as it is an easy consequence of a result of G. BIRKHOFF and O. FRINK).

(1) *I is the intersection of the prime ideals which contain it; in other words, I is the product of all its prime ideal divisors;*

(2) *I is the kernel of some representation.*

Proof. Firstly we verify that (1) implies (2). Let I be the intersection of all prime ideals which contain it, $I=\wedge P_\alpha$. There exists to every prime ideal P_α a congruence relation Θ_α with the property that[2]) $L(\Theta_\alpha)\cong \mathbf{2}$ and P_α is a congruence class under Θ_α. Obviously, the kernel of the congruence relation $\Theta=\wedge\Theta_\alpha$ is I. Hence it remains to prove that Θ is a representation, i. e. that $x\cup(y\cap z)\equiv(x\cup y)\cap(x\cup z)(\Theta)$. But this is evident, for $a\equiv b(\Theta)$ if and only if $a\equiv b(\Theta_\alpha)$ for all α.[3])

On the other hand, let I be the kernel of a representation Θ. The lattice $L(\Theta)$ is distributive and has zero element. Using Lemma I, for all $0\neq a\in L(\Theta)$ we may construct in $L(\Theta)$ a prime ideal which is disjoint to the dual ideal $[a)$. The meet of these prime ideals is the zero of $L(\Theta)$. I being the complete inverse image of the zero of $L(\Theta)$, the intersection of the complete inverse images of all above constructed prime ideals is I. By Lemma III, the complete inverse image of a prime ideal is again a prime ideal, so we get that I is the intersection of prime ideals. Qu. e. d.

Corollary 1. *Every ideal of a distributive lattice is the product of all its prime ideal divisors.*

Corollary 2. *Every maximal ideal of a distributive lattice is prime.*

(As a matter of fact these Corollaries are immediate consequences already of Lemma I, for any ideal I of the distributive lattice L is the meet of all P_α, $a\notin I$, if P_α is defined as a maximal ideal with $P_\alpha\supseteq I$, $a\notin P_\alpha$; by Lemma I any P_α is prime, hence the assertion follows.) Now we prove the converse of Corollary 1 of Theorem I.

Theorem II (Theorem 2.2 of [5]). *Each of the following conditions is necessary and sufficient in order that a lattice L be distributive:*

(1) *every ideal of L is the intersection of the prime ideals which contain it;*

(2) *every principal ideal of L is the intersection of the prime ideals which contain it;*

(3) *every ideal of L is the kernel of some homomorphism;*

(4) *every principal ideal of L is the kernel of some homomorphism.*

---

[2]) $L(\Theta)$ denotes the homomorphic image of L induced by Θ; $\mathbf{2}$ is the lattice of two elements. It is evident that in §§ 2—4 the whole lattice is considered as a prime ideal, but in §§ 5—9 it is not.

[3]) See [1], pp. 23—24.

Proof. With respect to Theorem I and to its Corollary 1, we need only prove that (4) implies the distrubitivity of L. If (4) is valid in L, but L is not distributive, then the latter fact implies that L has a sublattice isomorphic to the lattice of Fig. 1 or of Fig. 2. But in both cases the principal ideal $(a]$ is the kernel of no homomorphism. For, if we suppose that $(a]$ is a congruence class under the congruence relation Θ, then it follows $b = e \cap b = b \cap (a \cup c) \equiv b \cap (d \cup c) = b \cap c = d$ (Θ), but $b \notin (a]$, which is a contradiction.

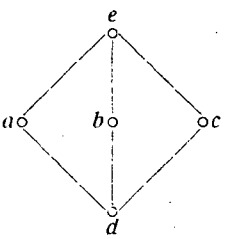

Fig. 1.

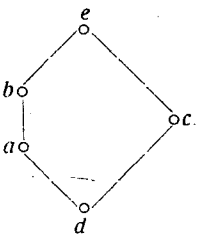

Fig. 2.

Corollary. *Let L be a lattice satisfying the ascending chain condition. L is distributive if and only if $(a]$ is prime for any meet-irreducible element a of L.*

Proof. In consequence of the ascending chain condition, every principal ideal is the meet of a finite number of principal ideals, generated by meet-irreducible elements. If we assume that every principal ideal with meet-irreducible generating element is prime, then we conclude that in L every principal ideal is the intersection of the prime ideals which contain it, i. e. by Theorem II, L is distributive. On the other hand if L is distributive and a is meet-irreducible, then as it is known, $(a]$ is prime (for if $x \cap y \in (a]$, then $a = (x \cap y) \cup a = (x \cup a) \cap (y \cup a)$, that is, $x \cup a = a$ or $y \cup a = a$, i. e. x or $y \in (a]$).

4. Characterization of the lattice of factorizable ideals.

In what follows $\mathfrak{L}$ denotes the lattice of all ideals of the lattice L.

Theorem III (Theorem 3.6 of [5]). *In case of a relatively complemented lattice L the ideals which are the intersections of prime ideals form a dual ideal $\mathfrak{A}$ of $\mathfrak{L}$.*

Proof. Let I be an ideal of the relatively complemented lattice L which is prime factorizable, that is, the intersection of the prime ideals which contain it and K, J two ideals of L with $K \supset J \supseteq I$. By Theorem I,

there exists a homomorphic image L' of L with kernel I, such that L' is distributive. We show that if K' and J' denote the homomorphic images of K and J, respectively, then under this homomorphism $K' \neq J'$. The case $J = I$ is trivial. If $J \supset I$, then let us choose three elements a, b, c such that $a \in K - J$ and $c \in J - I$,[4]) $b \in I$. Without loss of generality we may assume that $b < c < a$ (for $b < b \cup c < a \cup b \cup c$ and $b \cup c \in J - I$, $a \cup b \cup c \in K - J$). We denote by $\bar{c}$ any relative complement of c in the interval $[b, a]$. Then $\bar{c} \in K - J$, for in case $\bar{c} \in J$, $a = c \cup \bar{c} \in J$ would be valid too. Now if $K' = J'$, then with suitably chosen a and c, $a \equiv c$ would be valid. It follows $\bar{c} \equiv b$, that is, I would not be the kernel of this homomorphism.

Thus we have proved that every ideal which contains I is the complete inverse image of its homomorphic image in L'. As every ideal of L' is prime factorizable, the same is valid for all complete inverse images of them (see the proof of Theorem I).

On the other hand, if the ideals I and J are prime factorizable, then $I \cap J$ is obviously prime factorizable, completing the proof.

Corollary. *If a relatively complemented lattice has an element a such that both $(a]$ and $[a)$ are prime factorizable, then L is distributive.*

Proof. It is known that every convex sublattice of L is the set-theoretical intersection of an ideal I und a dual ideal J. If a convex sublattice contains a, then I contains $(a]$ and J contains $[a)$. It follows, by Theorem III, that I is prime factorizable. Consequently, by Theorem I, I is a congruence classe under some congruence relations. Dually we get that J has the same property. Hence, the set-theoretical intersection of I and J is also a congruence classe under a suitable congruence relation.

We obtain that every convex sublattice containing a is a congruence class under one and only one homomorphism. Thus this Corollary is a part of the following Theorem of [2] and [3]:

Le L be a lattice and x a fixed element in L. In order that every convex sublattice of L which contains x be a congruence class under one and only one congruence relation it is necessary and sufficient that L be distributive and every interval $[x, y]$ or $[y, x]$ as a sublattice be complemented.

---

[4]) $A - B$ denotes the set-theoretical difference of the sets A and B.

5. Uniqueness of factorization.

If $I=\bigwedge P_\alpha$, where every P_α is a prime ideal, then it is called a factorization of I (naturally we suppose that if $\alpha \neq \beta$ then $P_\alpha \neq P_\beta$).

Theorem IV (Theorem 4.1 of [5]). *Let L be any lattice and I an ideal of L. If I is represented as an intersection of a finite number of prime ideals, then its irredundant*[5]) *factorization is unique.*

Proof. Let

$$(*) \qquad I=P_1\cap P_2\cap\cdots\cap P_n=Q_1\cap Q_2\cap\cdots\cap Q_k$$

be two irredundant factorizations of I. Let us consider the ideal $J=Q_1\cap\cdots\cdots\cap Q_{i-1}\cap Q_{i+1}\cap\cdots\cap Q_k$. (We have supposed $k>1$. The case $n=k=1$ is obvious.) The factorizations (*) being irredundant, $J\supset I$, that is, there exists an $a\in J$ such that $a\notin I$. Consequently, for at least one index j, $a\notin P_j$. For any $q\in Q_i$ we have $q\cap a\in Q_i\cap J=I\subseteq P_j$, but $a\notin P_j$, therefore $q\in P_j$ (for P_j is prime), that is, $Q_i\subseteq P_j$. In a similar way may be proved the existence of some Q_m such that $P_j\subseteq Q_m$, that is, $Q_i\subseteq P_j\subseteq Q_m$. Since the factorizations (*) are irredundant, this is possible only in case $Q_i=P_j=Q_m$, that is if $i=m$. This at once implies that the two factorizations in (*) are the same.

In proving the Corollary of Theorem II we have seen that in a distributive lattice L a principal ideal $(a]$ is prime if and only if a is meet-irreducible (see [1], p. 142, too). Thus we have the following

Corollary. *In a distributive lattice L, the representation of an element as an irredundant meet of meet-irreducible elements is unique.*

Theorem V (Theorem 4.2 of [5]). *The following statements concerning a distributive lattice L are equivalent:*

(1) *L is relatively complemented;*

(2) *if an ideal of L is decomposed into the product of a finite number of its prime ideal divisors, then this factorization is unique;*

(3) *every prime ideal is maximal;*

(3′) *every dual prime ideal is maximal.*

Proof. (2) *implies* (3). If the prime ideal P is not maximal, then there exists an ideal I with $P\subset I\neq L$. By Lemma I there exists a prime ideal Q which contains I. Thus we get $P=P\cap Q$, i. e. the factorization of P is not unique.

---

[5]) The factorization in case $n>1$ is called irredundant if $P_1\cap\cdots\cap P_{i-1}\cap P_{i+1}\cap\cdots\cap P_n\supset I$ for all i.

(3) *implies* (1). Let $b < c < a$, and suppose that c has no relative complement in the interval $[b, a]$. Let us consider the dual ideal D, formed by the elements d, satisfying $d \cup c \geqq a$, and the dual ideal[6]) $E = (c] \cup D$. Obviously $b \notin E$, for in the contrary case $b = c \cap d$ (see footnote 6) for some $d \in D$, that is, d is a relative complement of c in $[b, a]$. So Lemma I may be used (for $I = (b]$ and E), that is, there exists a prime ideal P, such that P is disjoint to E and $b \in P$. At last we consider the ideal $(c] \cup P$. It is clear that a is not an element of $(c] \cup P$, for in the contrary case $a = c \cup p$ for some $p \in P$, hence by the definition of D, $p \in D$, contrary to the fact that P and E, and consequently, P and D are disjoint. According to Lemma I, there exists a prime ideal Q containing $(c] \cup P$ such that $a \notin Q$. By the definitions, Q properly contains P, that is, the prime ideal P is not maximal.

(1) *implies* (2). Let

$$(*) \qquad I = P_1 \cap \cdots \cap P_n = Q_1 \cap \cdots \cap Q_k$$

be two factorizations of the ideal I of the relatively complemented distributive lattice L. At first we show that these factorizations are irredundant. Indeed, if $I = P_2 \cap \cdots \cap P_n$, then by the distributivity of the lattice of all ideals of a distributive lattice (see [1], p. 141), $P_1 = P_1 \cup I = (P_1 \cup P_2) \cap \cdots \cap (P_1 \cup P_n)$, but every prime ideal in the lattice of all prime ideals of L is meet-irreducible (for, if P is a prime ideal and $P = I \cap J$, $P \neq I$, $P \neq J$, then let us choose an $x \in I - P$ and a $y \in J - P$; obviously, $x \cap y \in I \cap J = P$, a contradiction), hence for some i, $P_1 \cup P_i = P_1$, i. e. the prime ideal P_i is not maximal. By Theorem IV the two factorizations of I are the same, for in every relatively complemented distributive lattice all prime ideals are maximal (see [1], p. 160), that is, (1) implies (2).

Conditions (3) and (3′) are dual to each other, condition (1) is self-dual, consequently, (1) is equivalent to (3′) too, completing the proof.

Theorem VI (Lemma 4.3 of [5]). *If b covers a, then there exists at most one prime ideal P such that $a \in P$ and $b \notin P$. Accordingly, if n is the length of the shortest connected chain of the interval $[a, b]$, then there exist at most n prime ideals which contain a but not b.*[7])

Proof. Let us suppose that P and Q are prime ideals, $a \in P, Q$ and $b \notin P, Q$. If $P \not\supseteq Q$, then let us choose a $y \in Q - P$. Let $x = y \cup a \in Q - P$, so that $x \notin P$. Obviously, $b \cap x = a$, but $a \in P$, a contradiction.

---

[6]) The join of the dual ideals A and B is the dual ideal C generated by A and B. In distributive lattices (see [1], p. 141) any $c \in C$ is of the form $c = a \cap b$ $(a \in A, b \in B)$. Hence if $b \in [c) \cup D$, then $b = \bar{c} \cap d$ $(\bar{c} \geqq c, d \in D)$ and if, moreover, $b \leqq c$, then $b = c \cap b = c \cap \bar{c} \cap d = c \cap d$.

[7]) This is a somewhat sharpened form of Lemma 4.3 of [5]. We were unable to find in [5] the proof of the following Corollary.

Corollary. *In the lattice L, let n and m be the (finite) lengths of the shortest and the longest connected chains, respectively. Then L does not contain more than n prime ideals. L is distributive if and only if it contains m prime ideals.*

Proof. The first statement of the Corollary follows evidently from Theorem VI.

If L is a distributive lattice, and $1 = a_0 \succ a_1 \succ \cdots \succ a_m = 0$ ($x \succ y$ means that x covers y) is a (maximal) chain of length m, then, by Lemma I, for all i there exists a prime ideal which contains a_i, but not a_{i-1}. Consequently, in L there exist at least m prime ideals.

Conversely, let us suppose that L contains m prime ideals. These obviously separate (by Theorem VI) the chain $1 = a_0 \succ a_1 \succ \cdots \succ a_m = 0$ (i. e. for $i = 0, \ldots, m-1$ there exists a prime ideal P_{i+1} such that $a_i \notin P_{i+1}$, $a_{i+1} \in P_{i+1}$). By Theorem II, it is sufficient to prove that these separate all pairs of elements $y < x$. Let $1 = b_0 \succ b_1 \succ \cdots \succ b_n = 0$ be a maximal chain which is a refinement of $1 \geqq x > y \geqq 0$. Owing to Theorem VI in L there is at most n prime ideals. We have supposed the existence of precisely m prime ideals and we know that $n \leqq m$; it follows $n = m$ and the fact that every pair b_i, b_{i+1} ($i = 0, 1, \ldots, n-1$) is separated by some P_j. Thus, obviously, some P_j separates x and y too.

We have shown (Corollary 1 of Theorem I) that any ideal of a distributive lattice is the product of its prime ideal divisors. The following problem arises: in what lattices is every factorization unique?

Theorem VII (Theorem 4.3 of [5]). *The following statements concerning a lattice L are equivalent:*

(1) *every ideal of L is decomposed uniquely into the product of prime ideals;*

(2) *every principal ideal of L is decomposed uniquely into the product of prime ideals;*

(3) *$\mathfrak{L}$ is a relatively complemented distributive lattice;*

(4) *L is a relatively complemented distributive lattice in which every closed interval has a finite length.*

Proof. By Theorem II, any one of the conditions (1)—(4) implies the distributivity of the lattice L, hence it may be supposed without loss of generality that L is distributive.

(2) *implies* (1). Let us suppose, in contradiction to (1), that there exists an ideal I which is factorizable into prime divisors in two ways: $I = \bigwedge P_\alpha = \bigwedge Q_\beta$. Let a be an element of I and let us consider the (unique) factor-

ization of $(a] = \wedge R_\gamma$. Obviously $\wedge R_\gamma \cap \wedge P_\alpha$ and $\wedge R_\gamma \cap \wedge Q_\beta$ are (after omitting the R_γ equal to some P_α and Q_β, respectively) two different factorizations of $(a]$.

(1) *implies* (3). We consider ideals I and J such that $I \supset J$. Let $I = \wedge P_\alpha$ and $J = \wedge P_\alpha \cap \wedge P_\beta$ be the factorizations of I and J where all ideals P_β are different from all P_α. Consequently, $P_\beta \not\supseteq I$ for all P_β. We assert that $(\wedge P_\alpha) \cup (\wedge P_\beta) = L$. Indeed if $(\wedge P_\alpha) \cup (\wedge P_\beta) \neq L$, then there exists a prime ideal P which contains $(\wedge P_\alpha) \cup (\wedge P_\beta)$ and so $P \supseteq I$, therefore P is equal to some P_α, so P_α may be omitted from the factorization of J, in contradiction to (1). Hence every interval of the type $[J, L]$ is complemented, therefore $\mathfrak{L}$, which is distributive, is relatively complemented.

(3) *implies* (4). Let $b < a$ $(a, b \in L)$ and let I be an ideal such that $(a] \supset I \supset (b]$. From (3), I has a relative complement in the interval $[(b], (a]]$. Hence by Lemma II, I is a principal ideal, i. e. (4) is indeed proved to be true in L, for the interval $[b, a]$ of L — obviously — is a finite Boolean algebra in which every ideal is principal.[8])

(4) *implies* (2). Let $(a]$ be a principal ideal which has two different factorizations $(a] = \wedge P_\alpha = \wedge Q_\beta$. We choose an element $b > a$. Obviously, b is not element of all P_α and Q_β, e. g. let $b \notin P_1$ and $b \notin Q_1$. Combining condition (4) with Theorem V, we get that in L every prime ideal is maximal, hence $(b] \cup P_1 = (b] \cup Q_1 = L$. Since in a distributive lattice the relative complement is unique, we conclude $(b] \cap P_1 \neq (b] \cap Q_1$, furthermore $(b] \cap P_\alpha$ is a prime ideal in $(b]$. If we consider those elements of $\wedge((b] \cap P_\alpha)$ and $\wedge((b] \cap Q_\beta)$ which are in the interval $[a, b]$, we get obviously two different factorizations of the element a in the finite Boolean algebra $[a, b]$; this is clearly a contradiction.

6. Ideals and congruence relations.

According to Theorem II every ideal of a distributive lattice is a kernel of a suitable homomorphism. In general, it is possible that there exist more than one homomorphisms with the same kernel. G. BIRKHOFF proposed the following problem (see [1], p. 161):

Find necessary and sufficient conditions, in order that the correspondence between the congruence relations and ideals of a lattice be one-one.

---

[8]) See [1], p. 161, Ex. 3. We can prove it in the following way: If in the Boolean algebra B every ideal is principal, then every maximal ideal is also principal, that is, B is dually atomic, and hence atomic. The ideal I generated by the atoms of B, contains exactly those elements of B which are finite joins of the atoms of B, and the zero of B. I is a principal ideal, and the generating element x is a finite join of atoms. Obviously x is the greatest element of B and so B is finite.

This problem is answered in the following

Theorem VIII (Theorem 7.2 of [5]). *The congruence relations and the ideals of a lattice L correspond one-to-one if and only if L is a relatively complemented distributive lattice with* 0.

Proof. *Necessity.* The trivial (identical) homomorphism ought to have a kernel, hence 0 exists. The necessity of the distributivity is assured by Theorem II (condition (3)). At last, in order to verify the necessity of relative complementedness (we may already suppose that L is distributive), by Theorem V it is enough to prove that every prime ideal is maximal. But, in the contrary case there exist in L two prime ideals P and Q such that $P \subset Q$. It is evident that there exists a homomorphism with the kernel P, such that the homomorphic image is isomorphic to the lattice of two elements. On the other hand let $A_1 = P$, $A_2 = Q - P$, $A_3 = L - Q$. We define the relation Θ: $x \equiv y(\Theta)$ if and only if x and y are in the same A_i $(i = 1, 2, 3)$. It is easy to verify that Θ is a congruence relation; the homomorphism induced by Θ has the kernel P, and the homomorphic image is isomorphic to the chain of three elements. Consequently, P is the kernel of more than one homomorphism.

Sufficiency. This follows from Theorem II and from the evident fact that in a relatively complemented lattice with zero element every homomorphism is completely determined by its kernel ([1], p. 23).

9. Maximal extension of sublattices.

Generalizing a theorem of K. TAKEUCHI [6], J. HASHIMOTO proves that any sublattice of a relatively complemented distributive lattice may be extended to a proper, maximal one. In proving it he uses a lemma and by its aid he proves Theorem 9.1; both the lemma and the theorem are proved by making use of some topologies. The other parts of the proof have purely lattice-theoretical character. For this reason now we prove only Theorem 9.1 (we need not use the lemma).

Theorem IX (Theorem 9.1 of [5]). *Let a be an element of a distributive lattice L, which is neither* 0 *nor* 1, *and let S be a sublattice of L which does not contain a. Then there exist a prime ideal P and a dual prime ideal Q, such that (denoting by $P+Q$ the set-theoretical join of P and Q) $P+Q \supseteq S$ and $a \notin P+Q$.*

Proof. Let us consider (if it exists) the ideal I generated by those elements of S which are less than a. Obviously $a \notin I$, consequently, applying Lemma I for I and $[a)$, there exists a prime ideal P containing I but not

a. Now we consider the dual ideal D, generated by those elements of S which are not in P (if such elements exist). We prove that $a \notin D$. Indeed, $a \in D$ is equivalent to $a \geqq s \cap t$, where $s, t \in S$, but $s, t \notin P$. Since $a \notin S$, $a = s \cap t$ is impossible. Furthermore $a > s \cap t$ implies, by the definition of P, that $s \cap t \in P$, in contradiction to the prime property of P. Using again Lemma I, we may construct a dual prime ideal Q containing D but not a. P and Q fulfil the requirements.

If I is empty, then let P be any prime ideal not containing a. If D is empty then $P \supseteq S$, therefore Q may be an arbitrary dual prime ideal not containing a.

Added in proof. It escaped our attention that in his paper [5] J. HASHIMOTO also proves the following very interesting theorem (Theorem 8.5 of [5]) of purely lattice-theoretical character:

To any distributive lattice L there exists a generalized Boolean algebra B having the properties:

1. the lattice of all congruence relations of L is isomorphic to the lattice of all congruence relations of B;

2. L is a sublattice of B;

3. if the interval $[a, b]$ of L is of finite length, then $[a, b]$ has the same length as an interval of B.

HASHIMOTO devotes to the proof of this theorem an entire section in which he constructs B from L in a rather complicated topological way.

Recently we have succeeded in finding two simple proofs. One of these is an easy consequence of a construction of MAC NEILLE (Lattices and Boolean rings, *Bull. Amer. Math. Soc.*, **45** (1939), 453—455), while the other is based on the examination of the $\uparrow$-inaccessible elements of the lattice of all congruence relations of a lattice and uses some results of [3]. The second proof is also capable of some generalization.

Bibliography.

[1] G. BIRKHOFF, *Lattice theory*, Amer. Math. Soc. Coll. Publ., vol. 25, 2. ed. (New-York, 1948).

[2] GRÄTZER GY. és SCHMIDT E. T., Hálók ideáljai és kongruenciarelációi. I, II, *A Magyar Tud. Akadémia III. Osztályának Közleményei*, 7 (1957), pp. 93—109, 417—434.

[3] G. GRÄTZER and E. T. SCHMIDT, Ideals and congruence relations in lattices (to appear in *Acta Math. Acad. Sci. Hung.*).

[4] G. GRÄTZER and E. T. SCHMIDT, Characterizations of relatively complemented distributive lattices, *Publ. Math. Debrecen*, 5 (1957), 275—287.

[5] J. HASHIMOTO, Ideal theory for lattices, *Math. Japonicae*, 2 (1952), 149—186.

[6] K. TAKEUCHI, On maximal proper sublattices, *Journal Math. Soc. Japan*, 2 (1951), 228—230.

(Received October 17, 1957.)

On complete semi-groups.

By RICHARD WIEGANDT in Orosháza (Hungary).

§ 1.

By an (algebraic) structure we shall mean in the following a group, a ring or a semi-group. A structure will be called a T-structure if it has some specified additional property T.

It is a well-known fact that the Schreierian extensions of a group or a ring are the groups or rings, in which the given group or ring is a normal subgroup or an ideal, respectively. RÉDEI [3] treated the Schreierian extension theory of semi-groups with identity;[1]) the Schreierian extensions of a semi-group are the semi-groups in which it is a "left-normal semi-group" (see below).

Definition. A T-structure S is called *complete with respect to the property* T (shortly: T-complete) if it is a direct component (i. e. direct factor or direct summand) in every T-structure which is a Schreierian extension of S.

Examples of complete structures are the complete groups among the groups (each of their automorphisms is inner, their center consists of the identity only), the complete Abelian groups among the Abelian groups (for every element a and positive integer n there exists an element x such that $nx=a$), and the rings with identity among the rings. In these examples the property T means group, Abelian group, or ring, respectively (BAER [1], [2], RÉDEI [4]).

In this paper our main purpose is to characterize the complete regular semi-groups[2]) with identity; finally we make some remarks on groups and Abelian groups, which are complete with respect to certain properties.

---

[1]) A semi-group is a structure in which an associative multiplication is defined. The identity will be denoted always by e.

[2]) A semi-group is regular, when $xz=yz$ or $zx=zy$ implies $x=y$ for every element x, y, z.

§ 2.

Consider the case when the property T means "regular semi-group with identity". First we need some preparatory remarks.

Let F denote a semi-group with the identity e (F is not necessarily regular). According to RÉDEI [3], a sub-semi-group N of F is called left-normal, if F has a compatible classification of the form

$$a_1N,\ a_2N,\ldots \qquad (a_i \in F,\ a_1 = e) \tag{1}$$

and the products a_iN are without repetition.

Similarly we can define the right-normal semi-group. If N is at the same time left-normal and right-normal in F, then N is called a normal sub-semi-group of F.

Let us consider an example for a left-normal semi-group. Consider the semi-group which is generated by the elements e, a, b (e is the identity) and defined by the relation $ab = b$. It is easy to see that in this semi-group the elements e, a^n ($n \geqq 1$ integer) form a left-normal semi-group, but this left-normal semi-group is not right-normal.

Let b_i ($\in a_iN$) denote an arbitrary element of the class a_iN; then $b_iN \subseteq a_iN$ ($i = 1, 2, \ldots$), and the equality sign is valid obviously in every case if and only if N is a group.

N contains the identity of F. Otherwise we should have, according to the previous fact, $N = eN \subseteq a_kN$ ($a_k \neq e$) for some $k \neq 1$, what is impossible.

So F and N have a common identity, further a_k ($k = 2, 3, \ldots$) is contained in the class a_kN, but in general it is not possible to replace a_k by an arbitrary element of the class a_kN.

The classification (1) is determined uniquely by the semi-group N. Consider namely beside (1) an other left-normal classification

$$b_1N,\ b_2N,\ldots \qquad (b_1 = e) \tag{2}$$

of F. Every a_i belongs to a fixed b_kN, and b_k to a fixed a_lN. Since (2) is compatible, so $a_iN \subseteq b_kN$; from (1) follows $b_kN \subseteq a_lN$. Hence $a_iN \subseteq a_lN$, $a_iN = a_lN$ and $a_iN = b_kN$ follows proving the statement.

Lemma. *If N is normal in the semi-group F with identity, then the left-classes are identical with the right-classes. If a ($\in F$) has an inverse in F then the class of a can be written in the form aN, and we have $aN = Na$.*

Proof. Let a_kN be an arbitrary left-class and let a_k belong to the right-class Nb_l. Since the classification is compatible, so $a_k \equiv b_l$. Multiplying from the right with an arbitrary element r ($\in N$), we get

$$a_kr \equiv b_lr \equiv b_le \equiv b_l,$$

thus $a_kN \subseteq Nb_l$. Likewise $Nb_l \subseteq a_nN$; from these $k=n$ and $a_kN=Nb_l$ follows, which proves the first statement.

Let the element a $(\in F)$ have an inverse in F, and let a belong to the class a_kN. Then

$$aN \subseteq a_kN.$$

Multiplying from the left with a^{-1}, we get

$$N \subseteq a^{-1}a_kN.$$

Consequently in both relations the equality sign is valid and so the class of a is aN.

The third statement follows from the preceding statements.

Let the property T mean that the structure is a regular semi-group with identity. Such a semi-group is called complete by the above definition, if F is a direct factor of every regular semi-group with identity, which contains it as a left-normal semi-group.

Now we prove the following

Theorem. *The regular semi-group F with identity is complete if and only if its automorphisms are all inner automorphisms, and its center consists of the identity.*

Remark. If in particular F is a group, then the theorem reduces to a known theorem of BAER [1] for groups.

Proof. The proof is a modification of BAER's [1] proof.

Assume that F is complete, and let α be an arbitrary automorphism of F. Consider the factor-free Schreierian extension of F with an infinite[3]) cyclic group: $\bar{B} \approx I \circ F$ (I is the additive group of the integers). The elements of $\bar{B}$ are the pairs (i,f) $(i \in I, f \in F)$ in which the multiplication is defined by the following rule:

$$(i,f)(j,g)=(i+j, f^{\alpha^j}g)$$

(α^j is the j-th power of the automorphisms α).

By theorem 1 of RÉDEI [3] $\bar{B}$ is a semi-group, and $\bar{B}$ is obviously regular too. It is clear that $(0,e)$ is the identity of $\bar{B}$. In $\bar{B}$ the elements $(0,f)$ form a left-normal semi-group $\bar{F}$, which is isomorphic to F. Embed F in the usual way into $\bar{B}$; further denote the element $(1,e)$ by t, and denote the so formed semi-group by B. t has an inverse: $t^{-1}=(-1,e)$. Since

$$(i,f)=(1,e)^i(0,f),$$

the elements of B are of the form t^if. Since

$$(1,e)(0,f)(-1,e)=(0,f^\alpha),$$

---

[3]) If the order of the automorphism α is a finite number n, we may take instead of the infinite cyclic group, the cyclic group of order n.

the following relation holds in B:

$$tft^{-1} = f^{\alpha} \qquad (f \in F).$$

Thus the automorphism α of F is induced by the transformation of the element t ($\in B$). Since F is left-normal in B, therefore F is by the hypothesis a direct factor in B. Hence there exists an endomorphism β of B with the following properties:

$$B^{\beta} = F, \qquad f^{\beta} = f \qquad (f \in F).$$

In particular $s = t^{\beta} \in F$, and

i) there exists an inverse of s in F,

ii) for every element f in F

$$sfs^{-1} = t^{\beta} f (t^{\beta})^{-1} = (tft^{-1})^{\beta} = f^{\alpha\beta} = f^{\alpha}.$$

Thus the automorphism α is induced by the element s of F, thus every automorphism of F is inner.

Let z be an arbitrary element in the center of F. Denote by I' the additive semi-group of the non-negative integers, and consider the direct sum $J = I' + I'$. Consider the endomorphism-free Schreierian extension of F with J: $Z^* \approx J \circ F$. The elements of Z^* are of the form $((i,j),f)$ $((i,j) \in J, f \in F)$, and the multiplication is defined as follows:

$$((i,j),f)\,((k,l),g) = ((i+k, j+l), fgz^{jk}).$$

By theorem 1 of RÉDEI [3] Z^* is a semi-group, further Z^* is clearly regular. Obviously $((0,0),e)$ is the identity of Z^*. In Z^* the elements $((0,0),f)$ form a left-normal semi-group F^* which is isomorphic to F. Embed F into Z^* and denote the elements $((0,1),e)$, $((1,0),e)$ by x and by y, respectively. Denote the so formed semi-group by Z. It is easy to see that the following relations hold in Z:

$$xy = yxz, \quad xf = fx, \quad yf = fy \qquad (f \in F).$$

Since F is left-normal in Z, so F is by the hypothesis a direct factor in Z. Hence there exists an endomorphism γ of Z with the following properties:

$$Z^{\gamma} = F, \qquad f^{\gamma} = f \qquad (f \in F).$$

If $f \in F$ then

$$x^{\gamma} f = x^{\gamma} f^{\gamma} = (xf)^{\gamma} = (fx)^{\gamma} = fx^{\gamma},$$

which proves that x^{γ} belongs to the center of F. Analogously, y^{γ} belongs to the center of F. Consequently

$$y^{\gamma} x^{\gamma} = x^{\gamma} y^{\gamma} = (xy)^{\gamma} = (yxz)^{\gamma} = y^{\gamma} x^{\gamma} z^{\gamma}.$$

Since F is regular, we have $z = e$. Hence we have shown that the identity is the only element in the center of F; and so we have proved the necessity of the theorem.

Assume conversely that every automorphism of F is inner, and its center consists of the indentity only, further F is left-normal in the regular semi-group D with identity. Denote by C the centralizer of F in D (which consists of all those elements in D, which commute with every element in F).

We show that $CF = D$. Otherwise there would exist an element w ($\in D$) which does not belong to any class cF ($c \in C$). Let w belong to the class w_0F ($w_0 \notin C$). It may be assumed that w_0 has an inverse; otherwise we should consider the semi-group obtained by adjoining to D an element w_0^{-1} subjected to the following relation: $w_0^{-1}w_0 = e$; since D is regular, the obtained semi-group is an extension of F in which F is also left-normal. w_0 induces an automorphism of F, which contradicts the condition that every automorphism of F is inner. Consequently $D = CF$. Since $C \cap F = e$ according to the hypothesis, therefore D is the direct product of F and C. Hence F is direct factor in D, and this completes the proof.

§ 3.

Intermediate concepts between those of general groups and Abelian groups are the concepts of soluble groups and nilpotent groups. Consider the complete soluble and complete nilpotent groups. It is easy to see by the proof of the theorem that the center of a complete soluble or complete nilpotent (or other complete not Abelian) group must be the identity. On the other hand every soluble (and so every nilpotent) group has non-trivial center. So every complete soluble and complete nilpotent group must be the identity.

Every finitely generated complete Abelian group is the identity. They are namely the direct products of cyclic groups; but the cyclic groups are not direct factors in the containing cyclic groups.

The author is grateful to Professor L. RÉDEI who kindly helped him with the preparation of this paper.

Bibliography.

[1] BAER, R, Absolute retracts in group theory, *Bull. Amer. Math. Soc.*, **52** (1946), 501—506.

[2] BAER, R. Abelian groups that are direct summands of every containing Abelian group, *Bull. Amer. Math. Soc.*, **46** (1940), 800—806.

[3] RÉDEI, L., Die Verallgemeinerung der Schreierschen Erweiterungstheorie, *Acta Sci. Math.*, **14** (1952), 252—273.

[4] RÉDEI, L., Die Holomorphentheorie für Gruppen und Ringe, *Acta Math. Acad. Sci. Hung.*, **5** (1954), 169—195.

(Received September 29, 1957.)

Über die algebraischzahlentheoretische Verallgemeinerung eines elementarzahlentheoretischen Satzes von Zsigmondy.*)

Von LADISLAUS RÉDEI in Szeged.

Durchgängige Bezeichnungen und einige Benennungen:

„n" bezeichnet eine natürliche Zahl.

„ω" bezeichnet eine ganze algebraische Zahl.

„ω ist eine n-te Potenzzahl" soll bedeuten, daß ω die n-te Potenz eines Elementes des durch ω erzeugten Körpers ist. (Statt „n-te Potenzzahl" werde für $n=2, 3$ auch „Quadratzahl" bzw. „Kubikzahl" gesagt.)

„R" bezeichnet den Ring der ganzen rationalen Zahlen.

„R_ω" bezeichnet den Ring der ganzen Elemente des durch ω erzeugten Körpers. (Also $R_\omega = R$ für $\omega \in R$.)

„$\mathfrak{p}$" bezeichnet ein Primideal aus R_ω. (Üblicherweise werde stillschweigend $\mathfrak{p} \neq 0, R_\omega$ angenommen.) Diese Bezeichnung $\mathfrak{p}$ wird auch im Zusammenhang mit den unten zu definierenden $\omega_n, \omega_n^{(1)}, \ldots$ (statt ω) beibehalten.

„p" bezeichnet die durch $\mathfrak{p}$ teilbare Primzahl oder — wenn kein $\mathfrak{p}$ festgewählt wird — eine beliebige Primzahl.

„$N_\omega(\ldots), S_\omega(\ldots)$", kürzer „$N(\ldots), S(\ldots)$" bezeichnen die Norm eines Elementes oder Ideals bzw. die Spur eines Elementes von R_ω.

„$o(\ldots)$" bezeichnet die Ordnung $(=1, 2, \ldots, \infty)$ eines Elementes einer (multiplikativen) Gruppe (die stillschweigend auch Untergruppe irgendeiner vorgelegten algebraischen Struktur sein darf).

„$o(\omega(\mathrm{mod}\,\mathfrak{p}))$" bezeichnet für ein zu ω primes $\mathfrak{p}$ die Ordnung der Restklasse $\omega(\mathrm{mod}\,\mathfrak{p})$, anders die Ordnung von $\omega \bmod \mathfrak{p}$, d. h. das kleinste n mit $\omega^n \equiv 1 \,(\mathrm{mod}\,\mathfrak{p})$. (Man pflegt $o(\omega(\mathrm{mod}\,\mathfrak{p}))$ auch den Exponenten von $\omega \bmod \mathfrak{p}$ zu nennen.)

---

*) Erst nach der Fertigstellung des Manuskriptes dieser Arbeit wurde mir die Arbeit von H. Sachs, Untersuchungen über das Problem der eigentlichen Teiler, *Wiss. Zeitschrift d. Martin-Luther-Univ. Halle—Wittenberg*, **6**, Heft 2 (1956/57), 223—259 bekannt, in der ein allgemeineres Problem untersucht wird. Inhaltlich überschneiden sich beide Arbeiten nur sehr wenig.

„ω_n" bezeichnet ein ω mit unerfüllbarem $o(\omega \pmod{\mathfrak{p}}) = n$ und wird eine *exzeptionelle Zahl* (*für n*) genannt. Mehrere solche Zahlen werden auch mit $\omega_n^{(1)}, \omega_n^{(2)}, \ldots$ bezeichnet. Es ist klar, daß die Menge aller ω_n gegen Konjugiertenbildung invariant ist, weshalb konjugierte ω_n für gewöhnlich als nicht verschieden angesehen werden.

„a, b, c" bezeichnen Elemente von R.

„a_n, b_n" bezeichnen Elemente von R, deren sämtliche Primteiler in n aufgehen. Insbesondere bezeichnen also a_1, b_1 die Zahlen ± 1.

„Polynom" bedeutet hier stets ein Polynom über R.

„Hauptpolynom" bedeutet ein Polynom in einer Unbestimmten mit dem Anfangskoeffizienten 1.

„Grad..." bezeichnet den Grad einer algebraischen Zahl oder eines Primideals oder eines Polynoms.

„$f_\omega(x)$" bezeichnet das Minimalpolynom von ω, d. h. das irreduzible Hauptpolynom mit der Nullstelle ω. (Also ist Grad $f_\omega(x) = \text{Grad } \omega$.)

„ϱ" bezeichnet eine komplexe Zahl ($\neq 0$) mit $o(\varrho) = n$, d. h. eine primitive n-te komplexe Einheitswurzel.

„R_ϱ" bezeichnet also (als Spezialfall von R_ω) den Ring der ganzen Elemente des n-ten Kreisteilungskörpers.

„$F_n(x)$" bezeichnet das n-te Kreisteilungspolynom (ist also gleich $f_\varrho(x)$).

„$\varphi(n)$" ($= \text{Grad } \varrho = \text{Grad } F_n(x)$) bezeichnet die Eulersche Funktion.

„$\mu(n)$" bezeichnet die Möbiussche Funktion.

„$\mathfrak{p}^k \| \omega$" bezeichnet das Bestehen von $\mathfrak{p}^k | \omega$ und $\mathfrak{p}^{k+1} \nmid \omega$.

§ 1. Einleitung.

Wir beschäftigen uns mit den exzeptionellen Zahlen ω_n. Nach obiger Definition lassen sich diese auch so charakterisieren, daß $\omega_n^n - 1$ eine Einheit ist oder jeder Pimidealteiler von ihm schon in einem $\omega_n^d - 1$ ($d | n, < n$) aufgeht.

Die rationalen ω_n, d. h. die mit Grad $\omega_n = 1$, hat ZSIGMONDY [3] bestimmt. (Mit [ ] verweisen wir auf das Literaturverzeichnis am Schluß dieser Arbeit.) Sein diesbezüglicher interessanter Satz scheint sehr wenig bekannt zu sein und fand in der Literatur unseres Wissens bisher keine Anwendung. In einer anderen Arbeit [2] werden wir auf eine merkwürdige endlich-gruppentheoretische Folgerung dieses Satzes hinweisen. Hier untersuchen wir die ω_n bei beliebigem Grad ω_n und bekommen für sie weitgehende Aufklärungen, jedoch gelang uns ihre restlose Bestimmung nicht. Auf Grund unserer allgemeinen Resultate geben wir dann für den Satz von ZSIGMONDY einen neuen Beweis, der kürzer wird als der originale, ferner bestimmen wir die ω_n mit Grad $\omega_n = 2$ vollständig.

Satz 1. *Dann und nur dann ist* ω *ein* ω_n, *wenn* $F_n(\omega)$ *in einem* a_n *aufgeht.*

Korollar 1. *Sind* d, n *natürliche Zahlen und gehen alle Primteiler von* d *in* n *auf, so stimmen die* ω_{dn} *mit den* $\sqrt[d]{\omega_n}$ *überein.*

Da nämlich

$$F_{dn}(x) = F_n(x^d)$$

ist und die Zahlen a_{dn} mit den a_n übereinstimmen, so folgt Korollar 1 aus Satz 1.

Korollar 2. *Ist* n *ungerade, so stimmen die* ω_n *mit denjenigen* $-\omega_{2n}$ *überein, für die* $F_{2n}(\omega_{2n})$ *in einem* a_n *aufgeht.*

Da nämlich

$$F_{2n}(x) = F_n(-x)$$

ist, so folgt Korollar 2 aus Satz 1.

Man bemerke, daß das Problem der Bestimmung aller ω_n wegen Korollar 1 im wesentlichen auf den Fall von quadratfreien n zurückgeführt ist und man sich dabei wegen Korollar 2 auf die geraden n beschränken kann.

Korollar 3. *Eine komplexe Einheitswurzel* ω *ist dann und nur dann kein* ω_n, *wenn* $n \mid o(\omega)$ *gilt und* $\frac{o(\omega)}{n}$ $(\geqq 1)$ *die Potenz einer zu* n *primen Primzahl ist.*

Dem Beweis dieses Korollars schicken wir voraus, daß $\varrho - 1$ bekanntlich dann und nur dann keine Einheit ist, wenn $n = p^e$ $(e \geqq 0)$ ist, ferner gilt dann $(\varrho - 1, p) \neq 1$. Nunmehr berücksichtige man

$$F_n(\omega) = \prod_{\varrho} (\omega - \varrho),$$

wobei ϱ jetzt alle Einheitswurzeln mit $o(\varrho) = n$ durchläuft. Bis auf einen Einheitsfaktor stimmt die rechte Seite mit

$$\prod_{\varrho} (\omega \varrho^{-1} - 1)$$

überein. Nach voriger Bemerkung ist dieses Produkt offenbar dann und nur dann durch mindestens ein zu n primes Primideal teilbar, wenn die Bedingung von Korollar 3 erfüllt ist, weshalb dieses aus Satz 1 folgt.

Wegen

$$N_\omega(F_n(\omega))\,(= N_\omega(f_\varrho(\omega))) = (-1)^{\text{Grad}\,\omega\ \text{Grad}\,\varrho} N_\varrho(f_\omega(\varrho))$$

läßt sich Satz 1 auch so aussprechen:

Satz 1'. *Dann und nur dann ist ω ein ω_n, wenn $f_\omega(\varrho)$ in einem a_n aufgeht.*

Gleich zeigen wir, daß sich dieser Satz auch noch folgenderweise formulieren läßt:

Satz 1''. *Man nehme aus R_ϱ die in mindestens einem a_n aufgehenden Elemente, schreibe sie als $f(\varrho)$ mit Polynomen $f(x)$ vom Grad $< \varphi(n)$, lasse $g(x)$ alle Hauptpolynome durchlaufen und setze*

$$h(x) = g(x) F_n(x) + f(x).$$

Dann sind die (komplexen) Nullstellen der irreduziblen Polynome $h(x)$ und die der irreduziblen Hauptpolynome $f(x)$ eben die sämtlichen ω_n.

Die im Satz 1' genannte Bedingung läßt sich nämlich so aussprechen, daß das irreduzible Hauptpolynom $f_\omega(x)$ einem der im Satz 1'' genannten $f(x)$ mod $F_n(x)$ kongruent ist. Das beweist die Äquivalenz der Sätze 1', 1''.

Korollar 4. *Für jedes Paar n, k $(k = \varphi(n)+1, \varphi(n)+2, \ldots)$ gibt es unendlich viele ω_n mit Grad $\omega_n = k$.*

Denn nehme man ein $f(x)$ aus Satz 1''. Da $F_n(x)$ ein irreduzibles Hauptpolynom ist und $f(x) \neq 0$, Grad $f(x) <$ Grad $F_n(x)$ gelten, so ist

$$(x^l + z_1 x^{l-1} + \cdots + z_l) F_n(x) + f(x) \qquad (l = k - \varphi(n))$$

ein irreduzibles Element aus dem Polynomring $R[x, z_1, \ldots, z_l]$. Nach dem Irreduzibilitätssatz von HILBERT gewinnen wir also aus letzterem Polynom unendlich viele irreduzible Hauptpolynome k-ten Grades, indem wir $z_1, \ldots, z_l$ durch passende Elemente aus R ersetzen. Hieraus und aus Satz 1'' folgt somit Korollar 4.

Vermutung 1. Korollar 4 ist für $n > 1$, $k = \varphi(n)$ richtig.

Vermutung 2. Korollar 4 ist für $1 \leqq k < \varphi(n)$ falsch.

Über Vermutung 1 bemerken wir folgendes. Ist $p|n$, so wende man Satz 1'' mit $f(x) = p^t (t \geqq 0)$ und $g(x) = 1$ an. Es folgt, daß die Nullstellen derjenigen Polynome

$$F_n(x) + p^t,$$

die irreduzibel sind, lauter Zahlen ω_n mit Grad $\omega_n = \varphi(n)$ abgeben. In Hinsicht der Irreduzibilität darf man auf die Polynome

$$F_n(x+1) + p^t$$

übergehen. Da nun diese Polynome für $n = p^e (e \geqq 1)$, $t \geqq 2$ der Irreduzibilitätsbedingung von EISENSTEIN genügen, so folgt, daß Vermutung 1 für $n = p^e (> 1)$ richtig ist. Wir bemerken ferner, daß für $n = 2, 3, 4, 6$ nach den unten folgenden Sätzen 4, 5 beide Vermutungen richtig sind.

Eine wesentliche Verschärfung von Satz 1 liefert der folgende:

Satz 2. *Ist*

$$\mathfrak{p} \mid F_n(\omega_n), \tag{1}$$

weshalb nach Satz 1

$$n = p^e m,\ p^e \| n,\ e \geqq 1 \tag{2}$$

gesetzt werden kann, so gelten

$$m \mid p^{\text{Grad } \mathfrak{p}} - 1,\ o(\omega_n \pmod{\mathfrak{p}}) = m. \tag{3}$$

Besteht neben (1) *und* (2) *auch*

$$\mathfrak{p}^{\varphi(p^e)} \nmid p, \tag{4}$$

so geht $\mathfrak{p}$ *in* $F_n(\omega_n)$ *und* p *zu gleicher Potenz auf.*

Satz 3. *Die Anzahl der verschiedenen (rationalen) Primfaktoren von einem* $N(F_n(\omega_n))$ *ist je nach den Fällen Grad* $\omega_n \leqq 2$, *Grad* $\omega_n \geqq 3$ *höchstens gleich Grad* ω_n *bzw.* $-1 + \text{Grad } \omega_n$.

Satz 4. (ZSIGMONDY [3]). *Die sämtlichen rationalen* ω_n *sind*

$$\omega_1 = 2,\ \omega_2 = -1 + a_2,\ \omega_3 = -2,\ \omega_6 = 2,$$

außerdem noch $\omega_n = 0$ *für* $n = 1, 3, 4, 5, \ldots$, *ferner* $\omega_n = \pm 1$ *für* $n = 3, 4, 5, \ldots$.

Satz 5. *Die sämtlichen* ω_n *zweiten Grades sind*[1])[2])

$$\omega_1 = \frac{1}{2}(2 + a + \sqrt{a^2 + 4a_1}), \qquad S(\omega_1) = 2 + a, \qquad N(\omega_1) = 1 + a - a_1,$$

$$\omega_2 = \frac{1}{2}(-2 + a + \sqrt{a^2 + 4a_2}), \quad S(\omega_2) = -2 + a, \quad N(\omega_2) = 1 - a - a_2.$$

---

[1]) Die Fälle mit einer Quadratzahl unter dem Quadratwurzelzeichen sind außer Acht zu lassen; diese Ausnahmen sind (teils wegen Hilfssatz 11) offenbar die folgenden:

ω_1 für $a = \pm(1 - a_1)$;
ω_2 für $a = \pm(1 - a_2)$;
$\omega_3^{(1)}$ für $a_3 = -1, -3$; $\omega_3^{(2)}$ für $a_3 = 1, -3$; $\omega_3^{(3)}$ für $a_3 = -1, 3$; $\omega^{(4)}$ und $\omega^{(5)}$ für $a_3 = -1$; $\omega_3^{(6)}$ für $a_3 = \pm 1$
$\omega_4^{(1)}$ für $a_2 = 1, 2$; $\omega_4^{(2)}$ für $a_2 = \pm 2$; $\omega_4^{(3)}$ und $\omega_4^{(4)}$ für $a_2 = 1$;
$\omega_6^{(1)}$ für $a_6 = -1, -3$; $\omega_6^{(2)}$ für $a_6 = 1, -3$; $\omega_6^{(3)}$ für $a_6 = -1, 3$; $\omega_6^{(4)}$ und $\omega_6^{(5)}$ für $a_6 = -1$; $\omega_6^{(6)}$ für $a = \pm 1$.

[2]) Abgesehen von ganz einfachen Fällen haben wir im Satz 5 auch die Spur und Norm der exzeptionellen Zahlen $\omega_n, \omega_n^{(1)}, \ldots$ (d. h. im wesentlichen die Koeffizienten der definierenden Gleichungen dieser Zahlen) angegeben. Das wird den Beweis des Satzes bequemer machen. (Wir bemerken, daß man die exzeptionellen Zahlen von mindestens drittem Grade im allgemeinen gewiß durch ihre definierenden Gleichungen anzugeben zu bestreben hat.)

$$\begin{cases} \omega_3^{(1)} = \frac{1}{2}(-1+\sqrt{-3-4a_3}), & S(\omega_3^{(1)}) = -1, & N(\omega_3^{(1)}) = 1+a_3, \\ \omega_3^{(2)} = \frac{1}{2}(-1-a_3+\sqrt{-3+2a_3+a_3^2}), & S(\omega_3^{(2)}) = -1-a_3, & N(\omega_3^{(2)}) = 1, \\ \omega_3^{(3)} = \frac{1}{2}(-1-a_3+\sqrt{-3-2a_3+a_3^2}), & S(\omega_3^{(3)}) = -1-a_3, & N(\omega_3^{(3)}) = 1+a_3, \\ \omega_3^{(4)} = \frac{1}{2}(-1+a_3+\sqrt{(-3-6a_3+a_3^2}), & S(\omega_3^{(4)}) = -1+a_3, & N(\omega_3^{(4)}) = 1+a_3, \\ \omega_3^{(5)} = \frac{1}{2}(-1-a_3+\sqrt{(-3-6a_3+a_3^2}), & S(\omega_3^{(5)}) = -1-a_3, & N(\omega_3^{(5)}) = 1+2a_3, \\ \omega_3^{(6)} = \frac{1}{2}(-1-2a_3+\sqrt{(-3+4a_3^2}), & S(\omega_3^{(6)}) = -1-2a_3, & N(\omega_3^{(6)}) = 1+a_3, \end{cases}$$

$$\begin{cases} \omega_4^{(1)} = \sqrt{-1+a_2}, & & \\ \omega_4^{(2)} = \frac{1}{2}(a_2+\sqrt{-4+a_2^2}), & S(\omega_4^{(2)}) = a_2, & N(\omega_4^{(2)}) = 1 \\ \omega_4^{(3)} = \frac{1}{2}(a_2+\sqrt{-4+4a_2+a_2^2}), & S(\omega_4^{(3)}) = a_2, & N(\omega_4^{(3)}) = 1-a_2, \\ \omega_4^{(4)} = \frac{1}{2}(-a_2+\sqrt{-4+4a_2+a_2^2}), & S(\omega_4^{(4)}) = -a_2, & N(\omega_4^{(4)}) = 1-a_2, \end{cases}$$

$$\begin{cases} \omega_5^{(1)} = -1+\sqrt{-1}, \\ \omega_5^{(2)} = \frac{1}{2}(-3+\sqrt{5}), \end{cases}$$

$$\begin{cases} \omega_6^{(1)} = \frac{1}{2}(1+\sqrt{-3-4a_6}), & S(\omega_6^{(1)}) = 1, & N(\omega_6^{(1)}) = 1+a_6, \\ \omega_6^{(2)} = \frac{1}{2}(1+a_6+\sqrt{-3+2a_6+a_6^2}), & S(\omega_6^{(2)}) = 1+a_6, & N(\omega_6^{(2)}) = 1, \\ \omega_6^{(3)} = \frac{1}{2}(1+a_6+\sqrt{-3-2a_6+a_6^2}), & S(\omega_6^{(3)}) = 1+a_6, & N(\omega_6^{(3)}) = 1+a_6, \\ \omega_6^{(4)} = \frac{1}{2}(1-a_6+\sqrt{-3-6a_6+a_6^2}), & S(\omega_6^{(4)}) = 1-a_6, & N(\omega_6^{(4)}) = 1+a_6, \\ \omega_6^{(5)} = \frac{1}{2}(1+a_6+\sqrt{-3-6a_6+a_6^2}), & S(\omega_6^{(5)}) = 1+a_6, & N(\omega_6^{(5)}) = 1+2a_6, \\ \omega_6^{(6)} = \frac{1}{2}(1+2a_6+\sqrt{-3+4a_6^2}), & S(\omega_6^{(6)}) = 1+2a_6, & N(\omega_6^{(6)}) = 1+a_6, \end{cases}$$

$$\begin{cases} \omega_{10}^{(1)} = 1 + \sqrt{-1}, \\ \omega_{10}^{(2)} = \frac{1}{2}(3 + \sqrt{5}), \end{cases} \qquad \begin{cases} \omega_{12}^{(1)} = \sqrt{2}, \\ \omega_{12}^{(2)} = \frac{1}{2}(\pm 1 + \sqrt{5}), \\ \omega_{12}^{(3)} = \frac{1}{2}(\pm 3 + \sqrt{5}), \end{cases}$$

$$\omega_{20} = \frac{1}{2}(\pm 1 + \sqrt{5}), \qquad \omega_{24} = \frac{1}{2}(\pm 1 + \sqrt{5}),$$

außerdem noch die Einheitswurzeln $\sqrt{-1}$, $\frac{1}{2}(-1 + \sqrt{-3})$ *und* $\frac{1}{2}(1 + \sqrt{-3})$ *für* $n \neq 1, 4$ *bzw.* $n \neq 1, 3$, *bzw.* $n \neq 1, 2, 3, 6$.

§ 2. Beweis von Satz 1.

Um Satz 1 zu beweisen nehmen wir zuerst an, daß ω ein ω_n ist, und wollen zeigen, daß dann $F_n(\omega)$ Teiler eines a_n ist. Ist $F_n(\omega)$ eine Einheit, so ist das wahr. Im anderen Fall nehmen wir

$$\mathfrak{p} \mid F_n(\omega) \tag{5}$$

an. Noch mehr gilt dann

$$\mathfrak{p} \mid \omega^n - 1. \tag{6}$$

Wegen der Annahme folgt hieraus $o(\omega \pmod{\mathfrak{p}}) < n$, also die Existenz einer Primzahl q mit

$$q \mid n, \quad \mathfrak{p} \mid \omega^{\frac{n}{q}} - 1. \tag{7}$$

Da ferner

$$\frac{x^n - 1}{x^{\frac{n}{q}} - 1} \equiv q \pmod{x^{\frac{n}{q}} - 1} \tag{8}$$

besteht und die linke Seite durch $F_n(x)$ teilbar ist, so ergibt sich hieraus (bei der Ersetzung $x = \omega$) wegen (6) und (7_2) die Teilbarkeit $\mathfrak{p} \mid q$. Dies beweist wegen (7_1) die Behauptung, daß $F_n(\omega)$ in einem a_n aufgeht.

Umgekehrt, nehmen wir letzteres an. Wir haben zu zeigen, daß dann ω ein ω_n ist. Ist das falsch, so gibt es ein $\mathfrak{p}$ mit $o(\omega \pmod{\mathfrak{p}}) = n$. Dies bedeutet, daß (6) besteht und (7) für jede Primzahl q falsch ist. Wegen

$$\omega^n - 1 = \prod_{d \mid n} F_d(\omega), \qquad F_d(\omega) \mid \omega^d - 1$$

folgt hieraus die Erfülltheit von (5). Dies und die Annahme ergeben $\mathfrak{p} \mid n$, also

auch $p|n$. Hieraus, aus $p|N_\omega(\mathfrak{p})$ und aus dem Satz von FERMAT folgt

$$\omega^{\frac{n}{p}} \equiv \omega^{\frac{n}{p}N_\omega(\mathfrak{p})} \equiv 1 \pmod{\mathfrak{p}},$$

also $o(\omega(\mathrm{mod}\ \mathfrak{p})) < n$. Dies bedeutet, daß ω trotzdem ein ω_n ist. Mit diesem Widerspruch ist Satz 1 bewiesen.

§ 3. Beweis von Satz 2.

Hilfssatz 1. *Es sei $\alpha(\neq 1)$ ein Element von R_ω mit $\mathfrak{p}|\alpha-1$. Man setze*

$$\mathfrak{p}^k \| \alpha - 1, \qquad \mathfrak{p}^g \| p. \tag{9}$$

Gelten dann für eine natürliche Zahl e alle Ungleichheiten

$$\varphi(p^i)k \not\equiv g \qquad (i = 1, \ldots, e), \tag{10}$$

so gilt

$$\mathfrak{p}^{k_e} \| \alpha^{p^e} - 1 \tag{11}$$

mit

$$k_e = \min(p^e k, p^{e-1}k + g, p^{e-2}k + 2g, \ldots, k + eg). \tag{12}$$

Dem Beweis schicken wir voraus, daß offenbar

$$\min(pk_e, k_e + g) = k_{e+1} \tag{13}$$

und (wegen $\varphi(p)p^e = \varphi(p^{e+1})$)

$$\varphi(p)k_e = g \Longleftrightarrow \varphi(p^{e+1})k = g \tag{14}$$

gelten, wobei $\Longleftrightarrow$ für „dann und nur dann" steht.

Nunmehr beweisen wir Hilfssatz 1 zuerst für $e = 1$. Es gilt

$$\alpha^p - 1 = ((\alpha-1)+1)^p - 1 \equiv (\alpha-1)^p + p(\alpha-1) \pmod{p(\alpha-1)^2}. \tag{15}$$

Da ferner (10) für $e = 1$ als $(p-1)k \not\equiv g$, d. h. als $pk \not\equiv g + k$ lautet, so folgt aus (9) und (15)

$$\mathfrak{p}^{\min(pk,\, g+k)} \| \alpha^p - 1.$$

Der Exponent auf der linken Seite ist nach (12) gleich k_1, weshalb Hilfssatz 1 für $e = 1$ bewiesen ist.

Wir setzen dann Hilfssatz 1 für ein e voraus und beweisen ihn für $e+1$ wie folgt. Es sei (10) mit $e+1$ statt e erfüllt. Dies bedeutet das Erfülltsein von (10) selbst und wegen (14) das von $\varphi(p)k_e \not\equiv g$. Wegen des ersten und der Induktionsvoraussetzung besteht (11). Wegen des zweiten und der für $e = 1$ schon bewiesenen Richtigkeit von Hilfssatz 1 folgt also (mit Anwendung auf α^{p^e} statt α) das Bestehen von

$$\mathfrak{p}^{\min(pk_e,\, k_e+g)} \| \alpha^{p^{e+1}} - 1.$$

Wegen (13) ist hiermit Hilfssatz 1 allgemein bewiesen.

Hilfssatz 2. *Ist α ein Element von R_ω mit $\mathfrak{p}|\alpha-1$ und trifft*

$$\mathfrak{p}^{\varphi(p^e)} \nmid p \tag{16}$$

mit einem $e(\geqq 1)$ zu, so geht $\mathfrak{p}$ in

$$F_p(\alpha^{p^{e-1}}) \tag{17}$$

und p zu gleicher Potenz auf.

Im Fall $\alpha = 1$ ist (17) gleich p, weshalb jetzt die Behauptung trivial ist. Im übriggebliebenen Fall $\alpha \neq 1$ übernehmen wir die Bezeichnungen aus Hilfssatz 1. Wegen (9_2) läßt sich dann (16) als

$$\varphi(p^e) > g \tag{18}$$

schreiben.

Einerseits folgt hieraus

$$p^e k > p^{e-1}k + kg,$$

weshalb auf der rechten Seite von (12) sich das erste Glied streichen läßt, also

$$k_e = k_{e-1} + g \qquad (k_0 = k) \tag{19}$$

gilt.

Andererseits folgt aus (18) die Erfülltheit von (10), also nach Hilfssatz 1 die von (11) für alle $1, \ldots, e$ statt e. Letzteres und (9_1) besagen

$$\mathfrak{p}^{k_i} \| \alpha^{p^i} - 1 \qquad (i = 0, \ldots, e).$$

Man berücksichtige diese Relationen aber nur für $i = e, e-1$. Werden sie miteinander dividiert, so gewinnt man wegen (9_2) und (19) eben die Richtigkeit von Hilfssatz 2.

Nach diesen Vorbereitungen beweisen wir Satz 2. Um zuerst (3) zu beweisen setzen wir

$$m^* = o(\omega_n (\mathrm{mod}\ \mathfrak{p})), \text{ also } m^* | p^{\mathrm{Grad}\,\mathfrak{p}} - 1. \tag{20}$$

Dann braucht zur Bestätigung von (3) nur $m^* = m$ ausgewiesen zu werden.

Wegen (1) ist

$$\mathfrak{p} | \omega_n^n - 1. \tag{21}$$

Dies und (20_1) ergeben

$$m^* | n. \tag{22}$$

Andererseits bezeichne q einen von p verschiedenen Primteiler von n. Aus (1) und (8) folgt hierfür (bei der Ersetzung $x = \omega_n$)

$$\mathfrak{p} \nmid \omega_n^{\frac{n}{q}} - 1.$$

Hiernach und nach (20_1) ist

$$m^* \nmid \frac{n}{q}.$$

Dies besagt wegen (22), daß $\frac{n}{m^*}$ eine Potenz von p ist. Da ferner m^* wegen (20_2) zu p prim ist, so folgt wegen (2) die erhoffte Gleichheit $m^* = m$. Das beweist (3).

Um noch die andere Behauptung von Satz 2 zu beweisen setzen wir

$$\alpha = \omega_n^m. \tag{23}$$

Wendet man

$$\alpha \equiv \alpha^{N(\mathfrak{p})^k} (\mathrm{mod}\ \mathfrak{p})$$

mit genügend großem k an, so folgt aus (2), (21), (23) das Bestehen von $\mathfrak{p} | \alpha - 1$. Hieraus, aus (4) und (23) folgt nach Hilfssatz 2, daß $\mathfrak{p}$ in

$$F_n(\omega_n^{p^{r-1}m}) \tag{24}$$

und p zu gleicher Potenz aufgeht.

Nun entsteht aber aus

$$F_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$$

nach Abtrennung der zu $d = 1, p$ gehörenden Faktoren die Gleichung

$$F_n(x) = F_p(x^{\frac{n}{p}}) \prod_d{}' (x^{\frac{n}{d}} - 1)^{\mu(d)}, \tag{25}$$

wobei d die von 1, p verschiedenen quadratfreien Teiler von n durchzulaufen hat. Für diese ist $\frac{n}{d}$ wegen (2) kein Vielfaches von m, also ist für sie wegen der schon bewiesenen Beziehung (3_2)

$$\mathfrak{p} \nmid \omega_n^{\frac{n}{d}} - 1.$$

Wird also in (25) $x = \omega_n$ eingesetzt und (2) berücksichtigt, so besagt das über (24) Festgestellte eben die Richtigkeit der noch zu beweisenden Behauptung von Satz 2.

§ 4. Beweis von Satz 3.

Satz 3 ist richtig, wenn $F_n(\omega_n)$ eine Einheit ist. Im anderen Falle seien

$$p < p_2 < \cdots < p_k \qquad (k \geqq 1) \tag{26}$$

die verschiedenen Primteiler von $N(F_n(\omega_n))$, die also nach Satz 1 in n aufgehen.

Da insbesondere $(p, F_n(\omega_n)) \neq 1$ ist, so trifft (1) mit einem Primidealteiler $\mathfrak{p}$ von p zu, weshalb sich (2) wieder ansetzen läßt. Also besteht dann

$$p_2 \dots p_k | m.$$

Andererseits wenden wir aus Satz 2 jetzt nur (3_1) an. Hieraus und aus Vorigem folgt

$$p_2 \dots p_k | p^{\text{Grad}\,\mathfrak{p}} - 1.$$

Rechts darf wegen (26) durch $p-1$ dividiert werden. Wird dann „|" durch „$\leqq$" ersetzt, so hat man wieder wegen (26) und wegen $\text{Grad}\,\mathfrak{p} \leqq \text{Grad}\,\omega_n$

$$(1+p)^{k-1} \leqq 1 + p + p^2 + \dots + p^{-1+\text{Grad}\,\omega_n}.$$

Je nach den drei Fällen

$$\text{Grad}\,\omega_n = 1, = 2, \geqq 3$$

folgt hieraus der Reihe nach

$$k-1 = 0, \leqq 1, < -1 + \text{Grad}\,\omega_n,$$

d. h.

$$k = 1, \leqq 2, \leqq -1 + \text{Grad}\,\omega_n.$$

Da aber k eben die Anzahl der verschiedenen Primteiler von $N(F_n(\omega_n))$ bedeutet, so ist hiermit Satz 3 bewiesen.

§ 5. Beweis von Satz 4.

Hilfssatz 3. *Ist $n = p^e m$ mit $p^e \| n$, $e \geqq 1$ und α eine komplexe Zahl mit $|\alpha| > 1$, so gilt*

$$|F_n(\alpha)| \geqq \left(\frac{|\alpha|^{p^e} - 1}{|\alpha|^{p^{e-1}} + 1} \right)^{\varphi(m)}.$$

Da nämlich

$$F_n(\alpha) = F_m(\alpha^{p^e}) F_m(\alpha^{p^{e-1}})^{-1}, \qquad F_m(x) = \prod_{\sigma} (x - \sigma) \tag{27}$$

bestehen, wobei σ die $\varphi(m)$ komplexen Einheitswurzeln mit $o(\sigma) = m$ durchläuft, so folgt wegen $|\sigma| = 1$ die Richtigkeit von Hilfssatz 3.

Um Satz 4 zu beweisen betrachten wir ein ω_n mit

$$\text{Grad}\,\omega_n = 1. \tag{28}$$

Wir haben zu zeigen, daß diese ω_n eben die im Satz 4 aufgezählten sind.

Insbesondere lassen sich die ω_1 und ω_2 nach Satz 1 durch

$$(F_1(\omega_1) =)\, \omega_1 - 1 = a_1 \text{ bzw. } F_2(\omega_2) =)\, \omega_2 + 1 = a_2$$

charakterisieren. Diese bedeuten $\omega_1 = 1 + a_1 (= 1 \pm 1 = 2, 0)$ bzw. $\omega_2 = -1 + a_2$. Hiernach ist Satz 4 für $n = 1, 2$ richtig.

Trivial ist 0 für alle n ein ω_n, weshalb Satz 4 für $\omega_n = 0$ richtig ist. Ferner ist $\omega_n = 1$ bzw. $\omega_n = -1$ nach Korollar 3 genau für $n = 2, 3, 4, \ldots$ bzw. für $n = 1, 3, 4, \ldots$ erfüllt, also ist Satz 4 auch für $\omega_n = \pm 1$ richtig.

Wegen des Bewiesenen dürfen wir uns fortan auf den Fall

$$n \geqq 3, \quad |\omega_n| \geqq 2 \tag{29}$$

beschränken.

Wegen (28) lautet jetzt (3_1) als $m \mid p-1$. Hiernach folgt aus Satz 2, daß in $F_n(\omega_n)$ keine andere Primzahl als der größte Primteiler von n aufgehen kann. Fortan werde dieser mit p bezeichnet und

$$n = p^e m, \quad p^e \| n, \quad e \geqq 1 \tag{30}$$

gesetzt, wobei wegen (29_1)

$$p^e \geqq 3 \tag{31}$$

gilt. Da hiernach $\varphi(p^e) \geqq 2$, also (4) erfüllt ist, so folgt aus Satz 2 sogar

$$F_n(\omega_n) \mid p. \tag{32}$$

Andererseits sind wegen (29_2) und (30) die Voraussetzungen von Hilfssatz 3 mit $\alpha = \omega_n$ erfüllt. Aus diesem folgt wegen (29_2) und (31) noch mehr

$$|F_n(\omega_n)| > \left(\frac{1}{2}\,|\omega_n|^{\varphi(p^e)}\right)^{\varphi(m)} \geqq |\omega_n|^{(\varphi(p^e)-1)\varphi(m)} \tag{33}$$

Da stets $2^{p-1} \geqq p$ ist, so folgt aus (29_2), (32), (33)

$$(\varphi(p^e)-1)\varphi(m) \leqq p-2.$$

Dies ergibt wegen (31), daß im Fall der Existenz eines ω_n mit (28) und (29) notwendig

$$e = 1, \quad p \geqq 3, \quad \varphi(m) = 1 \tag{34}$$

gelten muß. Ferner folgt hieraus und aus (32), (33)

$$|\omega_n|^{p-2} < p. \tag{35}$$

Wegen (29_2) muß also $p \leqq 3$, somit wegen (34_2) $p = 3$ sein. Dies und $(34_{1,3})$ besagen, daß nur noch $n = 3, 6$ in Frage kommen, ferner folgt aus (29_2), (35) und $p = 3$, daß dabei notwendig $|\omega_n| = 2$, d.h. $\omega_n = \pm 2$ gelten muß.

Für die so übriggebliebenen insgesamt vier Möglichkeiten gelten (wegen $F_3(x) = x^2 + x + 1$, $F_6(x) = x^2 - x + 1$)

$$F_3(2) = 7, \quad F_3(-2) = 3, \quad F_6(2) = 3, \quad F_6(-2) = 7.$$

Satz 1 berücksichtigend sind wir also zum Schluß gekommen, daß die Bedingungen (28), (29) genau nur mit $\omega_3 = -2$, $\omega_6 = 2$ erfüllt sind. Dies mit den vor (29) erhaltenen Resultaten zusammen beweist Satz 4.

Der Leser sieht, daß in diesem Beweis aus Satz 1 im wesentlichen nur der Teil „nur dann“ und aus Korollar 3 nur ein trivialer Teil benutzt wurde, ferner sich der benutzte Teil von Satz 2 sich viel kürzer als selbst dieser Satz beweisen ließe.

§ 6. Erster Teil des Beweises von Satz 5.

Zum Beweis von Satz 5 haben wir die sämtlichen ω_n mit

$$\text{Grad } \omega_n = 2 \tag{36}$$

zu ermitteln. Der größeren Übersichtlichkeit halber spalten wir den Beweis in drei Teile auf, indem wir hier die quadratfreien geraden n, im § 7 die quadratfreien ungeraden n, im § 8 die übrigen n an die Reihe nehmen. Vorangehend erledigen wir aber gleich hier den Fall $|\omega_n| = 1$ und zwar für alle n.

Im Fall $|\omega_n| = 1$ ist ω_n wegen (36) nicht reell, also eine Einheitswurzel, und zwar kommen wieder wegen (36) nur

$$o(\omega_n) = 3, 4, 6$$

in Betracht. In diesen drei Fällen sind nach Korollar 3 die sämtlichen ungeeigneten n der Reihe nach die folgenden:

$$n = 1, 3 \quad \text{bzw.} \quad n = 1, 4 \quad \text{bzw.} \quad n = 2, 3, 6.$$

Die geeigneten n sind also zunächst in allen drei Fällen die $n = 5, 7, 8, 9, \ldots$, ferner noch einzeln in diesen drei Fällen der Reihe nach

$$n = 2, 4, 6 \quad \text{bzw.} \quad n = 2, 3, 6 \quad \text{bzw.} \quad n = 1, 4.$$

Das beweist Satz 5 für $|\omega_n| = 1$ und berechtigt uns fortan die Annahme

$$|\omega_n| \neq 1 \tag{37}$$

zu machen.[3])

Hilfssatz 4. *Ist $p \| n$, $n = pm$ und α eine komplexe Zahl mit $|\alpha| > 1$, so gilt*

$$|F_n(\alpha)| \geqq ((|\alpha| - 1)|\alpha|^{p-2})^{\varphi(m)}.$$

Da nämlich

$$|\alpha|^p - 1 \geqq |\alpha|^p - |\alpha|^{p-2} = (|\alpha| - 1)(|\alpha| + 1)|\alpha|^{p-2}$$

ist, so folgt Hilfssatz 4 aus Hilfssatz 3.

---

[3]) Einen Teil der gewünschten ω_n werden wir (wie auch in Satz 5) mit Formeln angeben, in denen a_2, a_3 oder a_6 als Variablen auftreten. Für einige ganz wenige Werte dieser Variablen wird dabei Grad $\omega_n = 1$ oder $|\omega_n| = 1$ ausfallen. Diese ω_n (für die also (36) oder (37) nicht zutrifft) werden stillschweigend außer Acht zu lassen, was hier ein für allemal bemerkt wurde.

Hilfssatz 5. *Ist* $p \| n, p \neq 2, n = pm$ *und* α *eine reelle Zahl mit* $|\alpha| < 1$, *so gilt*

$$|F_n(\alpha)| > \left(\frac{1}{2}\right)^{\varphi(m)}.$$

Dem Beweis schicken wir voran, daß für zwei reelle Zahlen u, v und eine komplexe Zahl σ mit

$$0 < u < v < 1, \quad |\sigma| = 1$$

stets

$$\left|\frac{u-\sigma}{v-\sigma}\right| > \frac{1}{2} \tag{38}$$

ist.

Bezeichnet nämlich σ' die zu σ konjugiert komplexe Zahl, so ist (38) gleichbedeutend mit

$$4(u^2-(\sigma+\sigma')u+1) > v^2-(\sigma+\sigma')v+1.$$

Es genügt dies für die beiden Extremalwerte $\sigma+\sigma' = \pm 2$ zu zeigen. Dabei handelt es sich um

$$4(u-1)^2 > (v-1)^2 \quad \text{und} \quad 4(u+1)^2 > (v+1)^2.$$

Das zweite ist trivial. Das erste ist gleichbedeutend mit $2(1-u) > 1-v$, d. h. mit $1+v > 2u$. Da dies zutrifft, so ist (38) bewiesen.

Aus (27) (angewendet mit $e = 1$) und aus (38) (angewendet mit $u = \alpha^p, v = \alpha$) folgt Hilfssatz 5 für positive α sofort. Da ferner (38) mit $-u, -v$ statt u, v richtig bleibt, so ist der Fall eines negativen α dem vorigen ähnlich.

Wir schicken noch voran, daß nach Satz 1 sich die ω_n als die ganzen algebraischen Zahlen mit

$$N(F_n(\omega_n)) = b_n \tag{39}$$

charakterisieren lassen. Da ferner für ein ω mit Grad $\omega = 2$ die Formel

$$\omega = \frac{1}{2}(S(\omega) + \sqrt{S(\omega)^2 - 4N(\omega)}) \tag{40}$$

gilt, so folgt, daß sich die ω_n mit Grad $\omega_n = 2$ auch durch

$$F_n(\omega_n) = \frac{1}{2}(a + \sqrt{a^2 + 4a_n}) \tag{41}$$

charakterisieren lassen. (Dabei wurde (39) mit $-a_n$ statt b_n angewendet, was ja gestattet ist, da beide dieselben Zahlen durchlaufen.)

Nach diesen Vorbereitungen wollen wir in diesem Paragraphen, wie gesagt, weiter nur die quadratfreien geraden n betrachten, und unterscheiden die Fälle $n = 2, n = 6, n > 6$.

Im Fall $n=2$ bekommen wir aus (41) wegen $F_2(x)=x+1$ die sämtlichen Lösungen unseres Problems in der Form

$$\omega_2=\frac{1}{2}(-2+a+\sqrt{a^2+4a_2}) \quad (\text{mit } N(F_2(\omega_2))=-a_2). \tag{42}$$

(Mit der hierbei in Klammern gesetzten Bemerkung haben wir spätere Zwecke.) Wegen (42) ist Satz 5 für $n=2$ richtig.

Im Fall $n=6$ nehmen wir die definierende Gleichung eines ω_6 bequemlichkeitshalber in der Form

$$\omega_6^2-(1+b)\omega_6+1+c=0 \tag{43}$$

an. Dann ist

$$F_6(\omega_6)=\omega_6^2-\omega_6+1=b\omega_6-c,$$

also (wieder wegen (43))

$$N(F_6(\omega_6))=b^2(1+c)-bc(1+b)+c^2=b^2-bc+c^2. \tag{44}$$

Somit besagt die Bedingung (39) für die ω_6 das Bestehen von

$$b^2-bc+c^2=b_6. \tag{45}$$

(Offenbar kommt dabei nur ein positives b_6 in Frage.)

Wir behaupten, daß die sämtlichen Lösungen b, c dieser Gleichung durch die Tabelle

(46)

b	0	a_6	a_6	$-a_6$	a_6	$2a_6$
c	a_6	0	a_6	a_6	$2a_6$	a_6
$N(F_6(\omega_6))$	a_6^2	a_6^2	a_6^2	$3a_6^2$	$3a_6^2$	$3a_6^2$

angegeben sind (wobei wir nach (44) jedesmal auch $N(F_6(\omega_6))$ berechnet haben).

Da nämlich die linke Seite von (45) homogen ist, so genügt es einzusehen, daß die der Bedingung $(b,c)=1$ unterworfenen zwölf („primitiven") Lösungen von (45) eben durch (46) mit $a_6=\pm 1$ geliefert sind. Das ist aber klar, da dann b_6 (>0) quadratfrei und ungerade, also nur 1 oder 3 sein kann, weshalb es sich jetzt um die b, c mit

$$b^2-bc+c^2=1 \quad \text{oder } 3$$

handelt. Somit ist die Behauptung über (46) bewiesen.

Nach (43) ist

$$\omega_6=\frac{1}{2}(1+b+\sqrt{(1+b)^2-4(1+c)}).$$

Werden hier b, c aus (46) eingesetzt, so entstehen eben die in Satz 5 aufgezählten $\omega_6^{(1)}, \ldots, \omega_6^{(6)}$. Somit ist dieser Satz für $n=6$ richtig.

Im Fall $n > 6$ bezeichnen wir mit p den maximalen Primteiler von n und setzen

$$n = pm, \tag{47}$$

wobei also (da n quadratfrei ist)

$$p \geqq 5,\ p \nmid m \tag{48}$$

gelten.

Dann zeigen wir vor allem, daß sich jetzt die ω_n als die ganzen algebraischen Zahlen mit

$$N(F_n(\omega_n)) \mid p^2 \tag{49}$$

charakterisieren lassen.

Wir haben nur zu zeigen, daß jetzt aus (39) das Bestehen von (49) folgt. Es genügt ein ω_n zu betrachten, wofür $N(F_n(\omega_n))$ keine Einheit ist. Wir bezeichnen mit p_0 einen Primteiler von dieser Norm. Wegen (39) muß $p_0 \mid n$ gelten, weshalb wir mit einer natürlichen Zahl m_0

$$n = p_0 m_0$$

setzen können, ferner hat p_0 nach der Annahme einen Primidealteiler $\mathfrak{p}_0$ mit

$$\mathfrak{p}_0 \mid F_n(\omega_n).$$

Wegen Grad $\mathfrak{p}_0 \leqq 2$ folgt aus Satz 2 zunächst

$$m_0 \mid p_0^2 - 1, \quad \text{d. h.} \quad m_0 \mid (p_0 - 1)(p_0 + 1).$$

Hieraus und aus (48_1) folgt (da p der maximale Primteiler von n ist), daß p kein Teiler von m_0 sein kann, d. h. notwendig

$$p_0 = p$$

ist. Indem wir entsprechend $\mathfrak{p}_0 = \mathfrak{p}$ setzen, so ist (4) (wieder wegen (48_1)) erfüllt, weshalb aus Satz 2 weiter folgt, daß $\mathfrak{p}$ in $F_n(\omega_n)$ und p zu gleicher Potenz aufgeht. Das hat (49) zur Folgerung, beweist somit die Behauptung.

Nunmehr wollen wir vor allem die nichtreellen ω_n bestimmen. Dann muß nach (49)

$$|F_n(\omega_n)| \leqq p$$

sein. Hieraus, aus (37), (47) und Hilfssatz 3 folgt

$$\left(\frac{|\omega_n|^p - 1}{|\omega_n| + 1}\right)^{\varphi(m)} \leqq p. \tag{50}$$

Hiernach und nach (48_1) muß noch mehr

$$\frac{|\omega_n|^5 - 1}{|\omega_n| + 1} \leqq 5$$

bestehen, weshalb $|\omega_n| < \sqrt{3}$[4]), d. h. $N(\omega_n) < 3$ ist. Dies und (37) ergeben

$$N(\omega_n) = 2, \quad \text{d. h.} \quad |\omega_n| = \sqrt{2}. \tag{51}$$

Da

$$\frac{(\sqrt{2})^{10} - 1}{\sqrt{2} + 1} > \frac{31}{3} > 10$$

ist, so folgt aus (50), (51) $p < 10$, also (wegen (48_1))

$$p = 5 \quad \text{oder} \quad p = 7.$$

Entsprechend lautet (50) wegen (51) als

$$(9 - 5\sqrt{2})^{\varphi(m)} \leqq 5 \quad \text{bzw.} \quad (17 - 9\sqrt{2})^{\varphi(m)} \leqq 7,$$

woraus $\varphi(m) < 4$ bzw. $\varphi(m) < 2$ folgt. Da aber m quadratfrei und gerade ist, so sind nur $m = 2, 6$ bzw. $m = 2$ möglich. Nach (47) kommen also nur

$$n = 10, 30, 14 \tag{52}$$

in Frage.

Andererseits läßt (51) nur die Fälle

$$\omega_n = \pm 1 + \sqrt{-1}, \quad \frac{1}{2}(\pm 1 + \sqrt{-7}) \tag{53}$$

zu. Unter den durch (52), (53) zugelassenen insgesamt 12 Möglichkeiten trifft aber (49) nach leichter Rechnung nur für den einzigen Fall $n = 10$, $\omega_{10} = 1 + \sqrt{-1}$ zu. Dies bedeutet, daß für ein quadratfreies gerades $n\,(> 6)$ nur ein einziges nichtreelles ω_n, nämlich

$$\omega_{10} = 1 + \sqrt{-1} \qquad (\text{mit } N(F_{10}(\omega_{10})) = 5) \tag{54}$$

existiert.

Wir haben noch die (49) befriedigenden reellen ω_n (für ein quadratfreies gerades $n > 6$) zu bestimmen. Man nehme ein solches ω_n an und bezeichne mit ω_n' sein Konjugiertes. Dabei darf

$$|\omega_n| \geqq |\omega_n'| \tag{55}$$

angenommen werden, woraus freilich

$$|\omega_n| > 1 \tag{56}$$

folgt. Wir unterscheiden zwei Fälle, je nachdem $|\omega_n'|$ kleiner oder größer als 1 ist.

Im Fall

$$|\omega_n'| < 1 \tag{57}$$

[4]) Wie hier so auch später fassen wir oft eine reelle Quadratwurzel stillschweigend als eine positive Zahl auf. Der Leser wird leicht sehen, wann das nötig ist.

gilt nach (47), (48), (49), (56) und den Hilfssätzen 3,5

$$\left(\frac{|\omega_n|^p-1}{2(|\omega_n|+1)}\right)^{\varphi(m)} < p^2. \tag{58}$$

Wegen (48$_1$) folgt hieraus

$$\frac{|\omega_n|^5-1}{2(|\omega_n|+1)} < 25,$$

also

$$|\omega_n| < 3. \tag{59}$$

Dies und (57) ergeben $|N(\omega_n)| < 3$, d. h. $|N(\omega_n)| = 1$ oder 2. Hieraus und aus (56), (59) folgt, daß nur

$$|\omega_n| = \frac{1}{2}(1+\sqrt{5}), \quad 1+\sqrt{2}, \quad 1+\sqrt{3}, \quad \frac{1}{2}(3+\sqrt{5})$$

in Frage kommen. Diese vier Fälle betrachten wir der Reihe nach.

Für

$$|\omega_n| = \frac{1}{2}(1+\sqrt{5}) \quad \text{(d. h.} \quad \omega_n = \pm\frac{1}{2}(1+\sqrt{5})\text{)}$$

hat man

$$\frac{|\omega_n|^{16}-1}{2(|\omega_n|+1)} > 16^2,$$

woraus wegen (58) $p < 16$, also wegen (48$_1$)

$$p = 5, 7, 11, 13$$

folgt. Wieder wegen (58) muß im ersten Fall $\varphi(m) < 5$ sein; da jetzt $5 \nmid m$, $2 | m$ ist, so hat man $m = 2$ oder 6. Im zweiten Fall folgt ähnlich $\varphi(m) < 4$, also wieder $m = 2$ oder 6. Im dritten und vierten Fall bekommt man $\varphi(m) < 2$, also $m = 2$. Somit kommen nach (47) nur

$$n = 10, 30, 14, 42, 22, 26$$

in Frage, jedoch trifft (49) nach leichter Rechnung in keinem dieser insgesamt 12 Fälle zu.

Für

$$|\omega_n| = 1+\sqrt{2} \quad \text{(d. h.} \quad \omega_n = \pm(1+\sqrt{2})\text{)}$$

hat man

$$\frac{|\omega_n|^7-1}{2(|\omega_n|+1)} > 7^2,$$

woraus wegen (58) $p < 7$, also $p = 5$ folgt, ferner ergibt sich aus (58) $\varphi(m) < 2$, $m = 2$, $n = 10$. Jedoch ist dabei (49) nicht erfüllt.

Für

$$|\omega_n| = 1+\sqrt{3} \qquad \text{(d. h.} \quad \omega_n = \pm(1+\sqrt{3})\text{)}$$

hat man

$$\frac{|\omega_n|^5-1}{2(|\omega_n|+1)} > 5^2,$$

weshalb jetzt sogar schon (58) mit keinem m erfüllt ist.

Für

$$\omega_n = \frac{1}{2}(3+\sqrt{5}) \qquad (\text{d. h. } \omega_n = \pm\frac{1}{2}(3+\sqrt{5}))$$

hat man

$$\frac{|\omega_n|^7-1}{2(|\omega_n|+1)} > 7^2,$$

woraus wegen (58) $p<7$, also $p=5$, und weiter hieraus $\varphi(m)<2$, $m=2$, $n=10$ folgt. Da

$$N\left(F_{10}\left(\frac{1}{2}(3+\sqrt{5})\right)\right)=5^2, \quad N\left(F_{10}\left(-\frac{1}{2}(3+\sqrt{5})\right)\right)=11^2$$

gelten, so ist (49) im ersten Fall erfüllt, im zweiten nicht erfüllt.

Wir haben bekommen, daß für ein quadratfreies gerades $n\,(>6)$ nur ein einziges, der Bedingung (57) unterworfenes reelles ω_n, nämlich

$$\omega_{10} = \frac{1}{2}(3+\sqrt{5}) \qquad (\text{mit } N(F_{10}(\omega_{10}))=5^2) \tag{60}$$

existiert.

Zu betrachten ist noch der Fall

$$|\omega_n'|>1. \tag{61}$$

Hieraus und aus (47), (49), (55) folgt nach Hilfssatz 3

$$\left(\frac{|\omega_n|^p-1}{|\omega_n|+1}\,\frac{|\omega_n'|^p-1}{|\omega_n'|+1}\right)^{\varphi(m)} \leqq p^2. \tag{62}$$

Genau so folgt nach Hilfssatz 4

$$((|\omega_n|-1)(|\omega_n'|-1)|\omega_n\omega_n'|^{p-2})^{\varphi(m)} \leqq p^2. \tag{63}$$

Wegen (55), (61) ist

$$|N(\omega_n)| = |\omega_n\omega_n'| \geqq 2.$$

Hiernach läßt sich

$$|\omega_n| = \frac{1}{2}(a+\sqrt{a^2\pm 4b}) \qquad (a\geqq 0,\ b\geqq 2) \tag{64}$$

ansetzen. Die beiden Fälle „$\pm$“ untersuchen wir getrennt.

Zuerst sei

$$|\omega_n| = \frac{1}{2}(a+\sqrt{a^2+4b}) \qquad \left(\text{also } |\omega_n'| = \frac{1}{2}(-a+\sqrt{a^2+4b})\right). \tag{65}$$

Dann folgt aus (61)

$$-a+\sqrt{a^2+4b}>2,\quad a^2+4b>(a+2)^2,\quad b>a+1,$$

also

$$a\leqq b-2. \tag{66}$$

Ferner lautet (63) wegen (65) als

$$((b+1-\sqrt{a^2+4b})b^{p-2})^{\varphi(m)}\leqq p^2. \tag{67}$$

(Freilich dürfte „=“ wegen der Irrationalität der linken Seite gestrichen werden.)

Wäre $b\geqq 4$, so folgte aus (48_1) und (67)

$$(b+1-\sqrt{a^2+4b})\,4^3<5^2.$$

Hiernach ist der erste Faktor kleiner als $\frac{1}{2}$, also folgt (teils aus (66))

$$\left(b+\frac{1}{2}\right)^2<a^2+4b\leqq b^2+4.$$

Dies ergibt $b+\frac{1}{4}<4$, $b<4$. Wegen dieses Widerspruchs muß $b\leqq 3$ sein.

Wenn $b=3$ ist, so folgt aus (66) $a\leqq 1$. Wegen (67) muß also

$$((4-\sqrt{13})3^{p-2})^{\varphi(m)}\leqq p^2$$

bestehen. Dies ergibt $p<7$, (wegen (48_1)) $p=5$, ferner $\varphi(m)<2$, $m=2$, somit (wegen (47)) $n=10$. Nach (65) kommen also jetzt für ω_n nur

$$\omega_{10}=\sqrt{3},\ \pm\frac{1}{2}(1+\sqrt{13})$$

in Frage. Jedoch ist (49) in diesen Fällen nicht erfüllt.

Im restlichen Fall $b=2$ muß wegen (66) $a=0$ sein. Hiernach und nach (65) ist

$$\omega_n=\pm\sqrt{2}.$$

Hierfür bekommt man aus (62)

$$\left(\frac{(\sqrt{2})^p-1}{\sqrt{2}+1}\right)^{\varphi(m)}\leqq p.$$

Dies ergibt zunächst $p<10$, also $p=5$ oder $p=7$. Ferner folgt für diese Fälle $\varphi(m)<3$, also $m=2, 6$ bzw. $\varphi(m)<2$, also $m=2$. Wegen (47) kommen somit nur $n=10, 30, 14$ in Frage. Jedoch ist dabei (49) nicht erfüllt. Somit haben wir die Möglichkeit (65) widerlegt.

Es bleibt noch aus (64) die andere Möglichkeit

$$|\omega_n|=\frac{1}{2}(a+\sqrt{a^2-4b}) \qquad (\text{also } |\omega_n'|=\frac{1}{2}(a-\sqrt{a^2-4b}) \tag{68}$$

zu untersuchen übrig. Wegen (61) muß dann

$$a-\sqrt{a^2-4b}>2,\ (a-2)^2>a^2-4b,\ -a+1>-b,$$

also

$$a \leqq b \tag{69}$$

sein. Ferner nimmt (63) wegen (68) die Form

$$((b+1-a)b^{p-2})^{\tau(m)} \leqq p^2.$$

an. Hieraus und aus (69) folgt

$$b^{p-2} \leqq p^2,$$

also (wegen (48_1)) $b<3$. Da aber $b \geqq 2$ ist, so folgt $b=2$. Dies mit (69) und $a \geqq 0$ zusammen widerspricht nach (68) der Reellität von ω_n.

Dies und die bei (54), (60) ausgesprochenen Resultate besagen, daß Satz 5 für die quadratfreien geraden $n(>6)$ richtig ist. Vereinigt mit den vorher erledigten Fällen $n=2, 6$ bedeutet das die Richtigkeit dieses Satzes für alle quadratfreien geraden n.

§ 7. Zweiter Teil des Beweises von Satz 5.

Auf Grund der eben erledigten Fälle beweisen wir jetzt Satz 5 für die quadratfreien ungeraden n mit Hilfe von Korollar 2. Nach diesem werden nämlich die ω_n für die gesagten n in der Form

$$\omega_n = -\omega_{2n} \tag{70}$$

erhalten, wobei rechts genau nur die ω_{2n} mit $N(F_{2n}(\omega_{2n}))=a_n$ und Grad $\omega_{2n}=2$ einzusetzen sind. Dabei kommen also nur die n mit $2n=2, 6, 10$, d. h. die $n=1, 3, 5$ in Frage.

Nun liefert diese Regel (70) angewendet mit $n=1, 3, 5$ (unter Berücksichtigung der bei (42), (46), (54), (60) hingestellten Normen) den Beweis von Satz 5 für diese n.

§ 8. Dritter Teil des Beweises von Satz 5.

Hilfssatz 6. *Ein ω mit Grad $\omega=2$ ist dann und nur dann eine Quadratzahl, wenn das Gleichungssystem*

$$y^2=N(\omega),\quad x^2=2y+S(\omega) \qquad (x, y \in R) \tag{71}$$

lösbar ist. Ist das der Fall, so liefern die Lösungen die sämtlichen Werte von $\sqrt{\omega}$ in der Form

$$\sqrt{\omega}=\frac{1}{2}(x+\sqrt{x^2-4y}). \tag{72}$$

Hilfssatz 7. *Ein ω mit Grad $\omega = 2$ ist dann und nur dann eine Kubikzahl, wenn das Gleichungssystem*

$$y^3 = N(\omega), \quad x^3 - 3xy = S(\omega) \qquad (x, y \in R) \tag{73}$$

lösbar ist. Ist das der Fall, so liefern die Lösungen die sämtlichen Werte von $\sqrt[3]{\omega}$ in der Form

$$\sqrt[3]{\omega} = \frac{1}{2}(x + \sqrt{x^2 - 4y}). \tag{74}$$

Diese zwei Hilfssätze sind Spezialfälle eines allgemeinen Satzes von uns [1]. Übrigens wird hier der zweite Teil von Hilfssatz 7 nicht benutzt.

Hilfssatz 8. *Es ist $1 + a_6$ genau nur für*

$$a_6 = -1, 3, 8, 24, 48, 288$$

eine Quadratzahl.

Denn es gibt unter den negativen a_6 offenbar nur die einzige Lösung $a_6 = -1$. Nachher sei $a_6 > 0$. Als Potenzen von 2 oder 3 sind bekanntlich genau nur $a_6 = 8$ bzw. $a_6 = 3$ passend. Nachher sei $6 | a_6$. Damit $1 + a_6$ eine Quadratzahl ist, muß dann sogar $8 | a_6$, also $24 | a_6$ sein. Wir setzen

$$1 + a_6 = 1 + 2^i 3^j = (1 + 6a)^2 \qquad (i \geqq 3, j \geqq 1)$$

an. Es folgt

$$2^{i-2} 3^{j-1} = a(1 + 3a).$$

Da unter den zwei Faktoren rechts der eine gerade, der andere ungerade ist, so muß im Fall $j = 1$ gewiß $a = \pm 1$ sein. Die entsprechenden Lösungen sind $a_6 = 7^2 - 1 = 48$ und $a_6 = (-5)^2 - 1 = 24$. Im Fall $j > 1$ muß

$$a = 3^{j-1} b, \quad 3 \nmid b, \quad 2^{i-2} = b(1 + 3^j b)$$

sein. Hieraus folgt $b = \pm 1$, also

$$\text{entweder } b = 1, \ 2^{i-2} = 1 + 3^j \quad \text{oder} \quad b = -1, \ 2^{i-2} = -1 + 3^j.$$

Da $j \geqq 2$ ist, so folgt im ersten Fall $i \geqq 5$, $8 | 1 + 3^j$, was offenbar unmöglich ist. Im zweiten Fall folgt ähnlich

$$i \geqq 4, \ 4 | -1 + 3^j, \ 2 | j; \ 2^{i-1} = (3^{\frac{j}{2}} + 1)(3^{\frac{j}{2}} - 1), \ 3^{\frac{j}{2}} - 1 = 2, \ j = 2, \ a = -3,$$

weshalb nur noch die Lösung $a_6 = (1 - 6 \cdot 3)^2 - 1 = 17^2 - 1 = 288$ entsteht. Das beweist Hilfssatz 8.

Hilfssatz 9. *Es ist $-1 + a_6$ genau nur für*

$$a_6 = 1, 2$$

eine Quadratzahl.

Denn aus $-1 + a_6 = a^2$ folgt sofort $3 \nmid a_6$, $4 \nmid a_6$, also $a_6 | 2$, ferner folgt $a_6 > 0$, weshalb nur $a_6 = 1, 2$ übrigbleiben.

Hilfssatz 10. *Es ist* $3+a_6$ *genau nur für*

$$a_6 = -3, -2, 1, 6$$

eine Quadratzahl.

Denn aus $3+a_6=a^2$ folgt sofort $4 \nmid a_6$, $9 \nmid a_6$, also $a_6 | 6$, ferner folgt $a_6 \geqq -3$. Hieraus entsteht die Behauptung leicht.

Hilfssatz 11. *Es ist* $-3+a_6$ *genau nur für*

$$a_6 = 3, 4, 12$$

eine Quadratzahl.

Denn aus $-3+a_6=a^2$ folgt sofort $8 \nmid a_6$, $9 \nmid a_6$, also $a_6 | 12$, ferner folgt $a_6 \geqq 3$. Hieraus entsteht die Behauptung.

Hilfssatz 12. *Es ist* $1+a_6$ *genau nur für*

$$a_6 = -9, -2, -1$$

eine Kubikzahl.

Denn aus

$$1+a_6=a^3$$

folgt $(a-1)(a^2+a+1)=a_6$, $a^2+a+1 | a_6$, also das Bestehen einer Gleichung

$$a^2+a+1=b_6.$$

Dies ergibt $(2a+1)^2=-3+4b_6$, also kommen nach Hilfssatz 11 nur

$$b_6 = 1, 3$$

in Frage. Das läßt für a nur die Möglichkeiten $a^2+a=0$ und $a^2+a=2$, d.h.

$$a = 0, -1, 1, -2$$

zu, von denen aber $a=1$ (wegen $a_6 \neq 0$) herausfällt. Hieraus und aus $a_6=-1+a^3$ folgt die Behauptung.

Hilfssatz 13. *Aus dem Bestehen von*

$$x^3-3x=1+a_6 \qquad (x \in R) \tag{75}$$

folgt das eine von $a_6 = -3, -1, 1$.

Denn die linke Seite von (75) ist gerade, also muß $2 \nmid a_6$ sein. Insbesondere für $a_6=3$ ist (75) offenbar unlösbar. Wenn somit die Behauptung falsch ist, so müßte (75) für mindestens ein a_6 mit $9 | a_6$ bestehen. Dann gälte

$$x^3-3x \equiv 1 \pmod 9.$$

Hierbei muß aber $x^3 \equiv 1 \pmod 3$, also $x \equiv 1 \pmod 3$, $x=1+3y$ $(y \in R)$ sein, woraus nach Einsetzung

$$(1+3y)^3-3(1+3y) \equiv 1 \pmod 9, \text{ d.h. } -3 \equiv 0 \pmod 9$$

folgt. Dieser Widerspruch beweist Hilfssatz 11.

Nunmehr wollen wir den Beweis von Satz 5 beenden. Zu bestimmen sind nur noch die ω_m mit Grad $\omega_m = 2$ für die natürlichen Zahlen m mit mehrfachen Primteilern. Korollar 1 liefert hierzu folgende Regel.

Man nehme die sämtlichen ω_n mit Grad $\omega_n \leqq 2$ und quadratfreiem $n(\geqq 2)$, bezeichne mit $d(\geqq 2)$ eine natürliche Zahl, deren alle Primteiler in n aufgehen, und suche die Fälle mit

$$\text{Grad } \sqrt[d]{\omega_n} = 2 \tag{76}$$

heraus; so entstehen eben die sämtlichen gewünschten ω_m in der Form

$$\omega_{dn} = \sqrt[d]{\omega_n} \tag{77}$$

Man bemerke, daß in dieser Regel nach Satz 4 und dem schon bewiesenen Teil von Satz 5 nur

$$n = 2, 3, 5, 6, 10 \tag{78}$$

in Frage kommen.

Insbesondere wenn $d = p$ $(p|n)$ ist, so kommen nur

$$d = p = 2, 3, 5 \tag{79}$$

in Betracht, aber wir zeigen vor allem. daß (76) für $p = 3, 5$ nicht befriedigt werden kann.

Denn betrachten wir zuerst den Fall

$$d = p = 3. \tag{80}$$

Nach (78) muß jetzt $n = 3$ oder 6 sein. Da nach Korollar 2 jedes ω_3 unter den $-\omega_6$ vorkommt, so genügt es (wegen Grad $\sqrt[3]{-\omega_6} =$ Grad $\sqrt[3]{\omega_6}$) unsere Behauptung für $n = 6$ zu beweisen. Wir haben auszuweisen, daß

$$\text{Grad } \sqrt[3]{\omega_6} = 2 \tag{81}$$

unmöglich ist, wenn hier für ω_6 die in den Sätzen 4, 5 aufgezählten Werte 2 und $\omega_6^{(i)}$ $(i = 1, \ldots, 6)$ eingesetzt werden.

Für $a_6 = 2$ ist das klar. Ferner besteht (81) nach Hilfssatz 7 für ein $\omega_6 = \omega_6^{(i)}$ dann und nur dann, wenn das Gleichungssystem

$$y^3 = N(\omega_6^{(i)}), \quad x^3 - 3xy = S(\omega_6^{(i)}) \qquad (x, y \in R) \tag{82}$$

lösbar ist. Nun lautet (82) (s. Satz 5) für $i = 1, \ldots, 6$ der Reihe nach als

$$(82^{(1)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1,$$

$$(82^{(2)}) \qquad y^3 = 1, \qquad x^3 - 3xy = 1 + a_6,$$

$$(82^{(3)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1 + a_6,$$

$$(82^{(4)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1 - a_6,$$

$$(82^{(5)}) \qquad y^3 = 1 + 2a_6, \qquad x^3 - 3xy = 1 + a_6,$$

$$(82^{(6)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1 + 2a_6.$$

Entsprechend unserer Behauptung werden wir zeigen, daß diese Gleichungssysteme $(82^{(i)})$ $(i=1,\ldots,6)$ jedesmal nur für solche Werte von a_6 lösbar sein können, für die das zugehörige $\omega_6^{(i)}$ entweder rational oder eine Einheitswurzel ist.

Aus dem Bestehen von $(82^{(1)})$ (sogar schon aus dem von $(82_2^{(1)})$) folgt $x|1, x^3\equiv 1 \pmod 3$, $x=1, y=0$. Hieraus und aus $(82_1^{(1)})$ folgt $a_6=-1$.

Aus $(82^{(2)})$ (sogar schon aus $(82_1^{(2)})$) folgt $y=1$. Hieraus und aus $(82_2^{(2)})$ folgt nach Hilfssatz 13 das eine von $a_6=-3, -1, 1$.

Aus $(82^{(3)})$ (sogar schon aus $(82_1^{(3)})$) folgt nach Hilfssatz 12, daß

(83) entweder $a_6=-9, y=-2$ oder $a_6=-2, y=-1$ oder $a_6=-1, y=0$

ist. Dabei geht $(82_2^{(3)})$ bzw. in

$$x^3+6x=-8,\quad x^3+3x=-1,\quad x^3=0 \tag{84}$$

über. Da hiervon nur die dritte Gleichung (in R) lösbar ist, so folgt $a_6=-1$.

Aus $(82^{(4)})$ schließt man ähnlich wie zuvor, die Abweichung ist, daß statt (84) der Reihe nach die drei Gleichungen

$$x^3+6x=10,\quad x^3+3x=3,\quad x^3=2$$

auftreten. Alle drei sind unlösbar, weshalb $(84^{(4)})$ für kein a_6 besteht.

Aus $(82^{(5)})$ (sogar schon aus $(82_1^{(5)})$) folgt nach Hilfssatz 12 $a_6=-1$.

Aus $(82^{(6)})$ schließt man ähnlich wie oben aus $(83^{(3)})$, die Abweichung ist, daß statt (84) der Reiche nach die drei Gleichungen

$$x^3+6x=-17,\quad x^3+3x=-3,\quad x^3=-1$$

auftreten. Da hiervon nur die dritte Gleichung möglich ist, so folgt wieder $a_6=-1$.

Man sieht hieraus tatsächlich, daß in den Gleichungssystemen $(82^{(i)})$ $(i=1,\ldots,6)$ jeweils nur solche a_6 möglich sind, für die das zugehörige $\omega_6^{(i)}$ entweder rational (vgl. hierzu[1])) oder eine Einheitswurzel ist. Das beweist, daß (76) im Fall (80) nicht befriedigt werden kann.

Dann haben wir den Fall

$$d=p=5 \tag{85}$$

zu betrachten. Für diesen erhalten wir das ähnliche Resultat sehr leicht. Jetzt kommen nach (78) nur $n=5$, 10 in Betracht. Da nach Korollar 2 jedes ω_5 unter den $-\omega_{10}$ vorkommt, so genügt es (wegen Grad $\sqrt[5]{-\omega_{10}}=$ Grad $\sqrt[5]{\omega_{10}}$) nur $n=10$ zu betrachten. Wir haben auszuweisen, daß

$$\text{Grad } \sqrt[5]{\omega_{10}}=2$$

nicht zutrifft, wenn für ω_{10} die Zahlen

$$\omega_{10}^{(1)} = 1 + \sqrt{-1}, \quad \omega_{10}^{(2)} = \frac{1}{2}(3 + \sqrt{3}) \tag{86}$$

aus Satz 5 eingesetzt werden. Das ist aber klar, da diese Zahlen keine 5-ten Potenzen sind. Somit haben wir bewiesen, daß (76) auch im Fall (85) nicht befriedigt werden kann.

Das bisherige bedeutet, daß die Anwendung unserer Regel unter den drei Fällen (79) nur im Fall $d = p = 2$ Zahlen von der Form (77) liefert. Freilich folgt hieraus sofort, daß in dieser Regel überhaupt unter allen d nur noch die

$$d = 2^e \qquad (e = 1, 2, \ldots) \tag{87}$$

in Betracht zu ziehen sind. Dabei kommen (unter allen Zahlen (78)) nur

$$n = 2, 6, 10 \tag{88}$$

in Frage. Diese drei Fälle betrachten wir einzeln.

Im Fall

$$n = 2 \tag{89}$$

bestimmen wir nach (77) zuerst die

$$\omega_4 = \sqrt{\omega_2}, \tag{90}$$

wobei nach (76) nur die ω_2 mit

$$\text{Grad } \sqrt{\omega_2} = 2 \tag{91}$$

zu berücksichtigen sind. Nach den Sätzen 4,5 kommen als solche nur die Zahlen

$$\omega_2 = -1 + a_2 \tag{92}$$

und

$$\omega_2 = \frac{1}{2}(-2 + a + \sqrt{a^2 + 4a_2}) \tag{93}$$

in Betracht. Für (92) ist (91) trivial erfüllt (ausgenommen wenn $-1 + a_2$ eine Quadratzahl, d.h. wenn $a_2 = 1$ oder 2 ist). Damit ferner (91) für (93) erfüllt ist, ist nach Hilfssatz 6 notwendig und hinreichend, daß das Gleichugssystem

$$y^2 = 1 - a - a_2, \quad x^2 = 2y - 2 + a \qquad (x, y \in R) \tag{94}$$

lösbar ist; selbst den Lösungen gehören dann nach demselben Hilfssatz vermöge (90) die

$$\omega_4 = \frac{1}{2}(x + \sqrt{x^2 - 4y}) \tag{95}$$

zu. Um die Lösungen von (94) zu bestimmen addieren wir die zwei Gleichungen dieses Systems:

$$x^2 + (y-1)^2 = -a_2.$$

Es genügt diese Gleichung zu lösen, da sich dann das passende a jedesmal aus (94_1) bestimmen läßt. Ihre sämtlichen Lösungen sind in der Tabelle

x	0	b_2	b_2	$-b_2$
y	$1-b_2$	1	$1-b_2$	$1-b_2$

angegeben. (Die entsprechenden Werte $-b_2^2$ bzw. $-2b_2^2$ von a_2 werden nicht gebraucht.) Werden diese x, y in (95) eingesetzt und a_2 für b_2 geschrieben, so entstehen eben die in Satz 5 mit $\omega_4^{(i)}$ $(i=1,\ldots,4)$ bezeichneten Zahlen. Da ferner die Einsetzung von (92) in (90) zu keinen neuen ω_4 (sondern wieder nur zu den $\omega_4^{(i)}$) führt, so ist hiermit Satz 5 für $n=4$ bewiesen.

Dann haben wir entsprechend dem Fall ($e=2$ d. h.) $d=4$ von (87) die ω_8 mit Grad $\omega_8=2$ zu bestimmen. Anstatt aber diese nach (77) in der Form $\omega_8=\sqrt[+]{\omega_2}$ anzusetzen, wollen wir sie auf Grund von Korollar 1 als

(96) $$\omega_8=\sqrt{\omega_4}$$

mit

(97) $$\text{Grad}\,\sqrt{\omega_4}=2$$

bestimmen, wobei die (eben bestimmten)

(98) $$\omega_4=\omega_4^{(i)} \qquad (i=1,\ldots,4)$$

aus Satz 5 in Betracht kommen. Es wird sich zeigen, daß überhaupt kein ω_8 mit Grad $\omega_8=2$ existiert, d. h. (97) für (98) nicht erfüllt ist. Wenn $i=1$ (d.h. $\omega_4=\omega_4^{(1)}=\sqrt{-1+a_4}$) ist, so ist das klar. Es bleiben die Fälle $i=2,3,4$ zu untersuchen übrig. Wegen Hilfssatz 6 haben wir zu zeigen, daß die drei Gleichungssysteme

$$y^2=N(\omega_4^{(i)}),\ x^2=2y+S(\omega_4^{(i)}) \qquad (i=2,3,4)$$

keine passenden Lösungen $x, y(\in R)$ haben. Diese Gleichungssysteme lauten (nach Satz 5) der Reihe nach als

(99) $$y^2=1, \qquad x^2=2y+a_2,$$

(100) $$y^2=1-a_2, \qquad x^2=2y+a_2,$$

(101) $$y^2=1-a_2, \qquad x^2=2y-a_2.$$

Offenbar hat (99) nur die Lösungen

$$y=1,\ x=0;\ y=1,\ x=\pm 1;\ y=1,\ x=\pm 2;\ y=-1,\ x=0,$$

ferner hat (100) nur die Lösungen

$$y=0,\ x=\pm 1,$$

endlich hat (101) überhaupt keine Lösungen. Werden nun die gefundenen

$$\frac{1}{2}(x+\sqrt{x^2-4y})$$

eingesetzt, so entstehen lauter Einheitswurzeln. Das beweist auf Grund des zweiten Teils von Hilfssatz 6 die Behauptung, daß keine ω_n mit Grad $\omega_n = 2$ existieren. Freilich folgt hieraus ähnliches für ω_{2^k} $(k \geqq 4)$ statt ω_n. Somit ist Satz 5 für $n = 2^k$ $(k \geqq 3)$ bewiesen.

Im Fall

(102) $$n = 6$$

bestimmen wir nach (77) zuerst die

(103) $$\omega_{12} = \sqrt{\omega_6},$$

wobei nach (76) nur die ω_6 mit

(104) $$\text{Grad}\sqrt{\omega_6} = 2$$

einzusetzen sind. Nach den Sätzen 4,5 kommen als solche nur die Zahlen

(105) $$\omega_6 = 2$$

und

(106) $$\omega_6 = \omega_6^{(i)} \qquad (i = 1, \ldots, 6)$$

in Betracht. Für (105) ist (104) trivial erfüllt. Damit ferner (104) für (106) erfüllt ist, ist nach Hilfssatz 6 notwendig und hinreichend, daß das Gleichungssystem

$$y^2 = N(\omega_6^{(i)}),\ x^2 = 2y + S(\omega_6^{(i)}) \qquad (x, y \in R)$$

lösbar ist. Selbst die zugehörigen ω_{12} entstehen nach Einsetzung der Lösungen x, y in

(107) $$\omega_{12} = \frac{1}{2}(x + \sqrt{x^2 - 4y}).$$

Nun handelt es sich nach Satz 5 der Reihe nach für $i = 1, \ldots, 6$ um die folgenden Gleichungssysteme:

$$\begin{aligned}
&y^2 = 1 + a_6, && x^2 = 2y + 1,\\
&y^2 = 1, && x^2 = 2y + 1 + a_6,\\
&y^2 = 1 + a_6, && x^2 = 2y + 1 + a_6,\\
&y^2 = 1 + a_6, && x^2 = 2y + 1 - a_6,\\
&y^2 = 1 + 2a_6, && x^2 = 2y + 1 - a_6,\\
&y^2 = 1 + a_6, && x^2 = 2y + 1 + 2a_6.
\end{aligned}$$

Die in Frage kommenden Werte von a_6 erhält man aus Hilfssatz 8. ausgenommen das zweite Gleichungssystem, bei dem man zu diesem Zweck der Hilfssätze 9,10 bedarf. So bekommt man leicht, daß die ersten drei Gleichungssysteme der Reihe nach nur die Lösungen

$$y = 0,\ x = \pm 1;$$

$$y = 1,\ x = 0,\ \pm 1,\ \pm 2,\ \pm 3;\ y = -1,\ x = 0,\ \pm 1;$$

$$y = 0,\ -2,\ x = 0$$

haben, dagegen die übrigen drei unlösbar sind. Die Einsetzung dieser

Lösungen in (107) liefert (Einheitswurzeln und rationale Zahlen bei Seite gelassen) die folgenden Zahlen:

$$(108) \qquad \omega_{12} = \frac{1}{2}(\pm 3 + \sqrt{5}),\ \frac{1}{2}(\pm 1 + \sqrt{5}),\ \sqrt{2}.$$

Da diese auch schon den aus (103), (105) entspringenden Fall $\omega_{12} = \sqrt{2}$ umfassen und mit den $\omega_{12}^{(i)}$ $(i = 1, 2, 3)$ in Satz 5 übereinstimmen, so ist dieser Satz für $n = 12$ bewiesen. Da ferner unter diesen Zahlen (108) nur die $\omega_{12} = \frac{1}{2}(\pm 3 + \sqrt{5})$ Quadratzahlen sind, so folgt (aus Korollar 1) auch, daß die sämtlichen ω_{24} mit Grad $\omega_{24} = 2$ die

$$(109) \qquad \omega_{24} = \sqrt{\omega_{12}} = \frac{1}{2}(\pm 1 + \sqrt{5})$$

sind. Das beweist Satz 5 für $n = 24$. Da endlich diese Zahlen (109) keine Quadratzahlen sind, so folgt ähnlich, daß keine ω_{48} mit Grad $\omega_{48} = 2$ vorhanden sind, weshalb Satz 5 für $n = 48$ richtig ist. Freilich folgt ähnliches für alle $n = 2^k 3$ $(k \geqq 5)$.

Endlich ist aus (88) nur noch der Fall

$$n = 10$$

übrig. Jetzt kommen wir ähnlich aber schnell zum Ziel. Wir betrachten die Zahlen

$$\omega_{10}^{(1)} = 1 + \sqrt{-1},\ \omega_{10}^{(2)} = \frac{1}{2}(3 + \sqrt{5})$$

aus Satz 5. Unter diesen ist nur die zweite eine Quadratzahl, weshalb die sämtlichen ω_{20} mit Grad $\omega_{20} = 2$ die

$$\omega_{20} = \sqrt{\omega_{10}^{(2)}} = \frac{1}{2}(\pm 1 + \sqrt{5})$$

sind. Das beweist Satz 5 für $n = 20$. Da endlich ω_{20} keine Quadratzahl ist, so folgt, daß keine ω_{40} mit Grad $\omega_{40} = 2$ vorhanden sind, weshalb Satz 5 für $n = 40$ richtig ist. Ähnliches folgt für alle $n = 2^k 5$ $(k \geqq 4)$. Hiermit ist der Beweis von diesem Satz beendet.

Literaturverzeichnis.

[1] L. Rédei, Potenzelemente in Körpern. (Erscheint später in den *Acta Math. Acad. Sci. Hung.*)

[2] L. Rédei, Eine Bemerkung über die endlichen einstufig nichtkommutativen Gruppen, *Acta Sci. Math.*, **19** (1958), 127—128.

[3] L. Zsigmondy, Zur Theorie der Potenzreste, *Monatshefte f. Math.*, **3** (1892), 265—284.

(Eingegangen am 1. September 1957.)

Eine Bemerkung über die endlichen einstufig nichtkommutativen Gruppen.

Von LADISLAUS RÉDEI in Szeged.

Einstufig nichtkommutativ heißt eine Gruppe, die nur kommutative echte Untergruppen hat, ohne selbst kommutativ zu sein. Ob es unter ihnen auch unendliche Gruppen gibt, ist unbekannt. Die endlichen Gruppen dieser Art sind vollständig bekannt.[1]) Sie sind teils p-Gruppen, teils haben sie eine durch genau zwei verschiedene Primzahlen teilbare Ordnung. Die letzteren Gruppen haben stets genau nur eine normale Sylowgruppe. Diese ist freilich kommutativ, außerdem ist sie elementar, worunter wir verstehen, daß ihre Elemente ($\neq 1$) von Primzahlordnung sind.

Die Frage wurde bisher nicht aufgeworfen, ob jede endliche kommutative elementare Gruppe die normale Sylowgruppe von mindestens einer endlichen einstufig nichtkommutativen Gruppe ist.

Satz. *Eine endliche kommutative elementare Gruppe ist dann und nur dann die normale Sylowgruppe von mindestens einer endlichen einstufig nichtkommutativen Gruppe, wenn ihre Ordnung weder* 2 *noch* 2^6 *noch das Quadrat einer Mersenneschen Primzahl*[2]) *ist.*

Dieser Satz wird als Folgerung aus[1]) und aus einem elementarzahlentheoretischen Satz von K. ZSIGMONDY entstehen (s. unten).

Nach[1]) gewinnt man nämlich diejenigen endlichen einstufig nichtkommutativen Gruppen, die keine p-Gruppen sind, folgenderweise. Man nehme ein beliebiges (geordnetes) Tripel

$$p, q, r \tag{1}$$

bestehend aus zwei verschiedenen Primzahlen p, q und einer natürlichen Zahl

---

[1]) L. RÉDEI, Das „schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören, *Commentarii Math. Helv.*, **20** (1947), 225—264.

[2]) Die Mersenneschen Primzahlen sind diejenigen von der Form $2^q - 1$ (q Primzahl).

r. Man setze

$$u = o(p(\mathrm{mod}\, q)), \tag{2}$$

worunter wir verstehen, daß u die Ordnung der Restklasse $p(\mathrm{mod}\, q)$, d. h. die kleinste natürliche Zahl mit $p^u \equiv 1(\mathrm{mod}\, q)$ ist. Man bezeichne mit K den (endlichen) Körper von der Ordnung

$$O(K) = p^u, \tag{3}$$

führe in der Menge der $p^u q^r$ Symbole

$$P_\alpha Q^i \qquad (\alpha \in K;\ i = 0, \ldots, q^r - 1)$$

die Multiplikation

$$P_\alpha Q^i \cdot P_\beta Q^k = P_{\alpha + \omega^i \beta} Q^{(i+k)} \tag{4}$$

ein, wobei $(i+k)$ den kleinsten nichtnegativen Rest von $i+k \bmod q^r$ und ω ein festgewähltes Element $(\neq 0)$ von K von der Ordnung

$$o(\omega) = q$$

bezeichnet. (Da aus (2) $q \mid p^u - 1$ folgt, so gibt es wegen (3) genau $q-1$ solche ω.) Es wird durch (4) eine einstufig nichtkommutative Gruppe G von der Ordnung

$$O(G) = p^u q^r$$

definiert, dabei hängt G (bis auf Isomorphie) nur vom Tripel (1) an, dagegen sind die zu den verschiedenen Tripeln (1) gehörenden G paarweise wesentlich verschieden und erschöpfen alle endlichen einstufig nichtkommutativen Gruppen, die keine p-Gruppen sind. Man sieht aus (4) auch, daß die Elemente P_α die (normale) p-Sylowgruppe von G bilden und diese zur additiven Gruppe der Elemente von K isomorph ist. (Da G direkt unzerlegbar ist, so folgt hieraus schon, daß die q-Sylowgruppen nicht normal sein können.) Hiernach ist die normale Sylowgruppe von G kommutativ und elementar, ferner ist ihre Ordnung wegen (3) gleich p^u.

Andererseits ist (2) bei gegebenen p, u nach dem Satz von ZSIGMONDY[3]) dann und nur dann mit keinem q erfüllbar, wenn p^u gleich 2 oder 2^6 oder das Quadrat einer Mersenneschen Primzahl ist. Somit ist unser Satz bewiesen.

(Eingegangen am 20. Januar 1958.)

[3]) Siehe K. ZSIGMONDY, Zur Theorie der Potenzreste, *Monatshefte f. Math.*, **3** (1892), 265—284 oder L. RÉDEI, Über die algebraischzahlentheoretische Verallgemeinerung eines elementarzahlentheoretischen Satzes von Zsigmondy, *Acta Sci. Math.*, **19** (1958), 98—126.

Bemerkungen über den Maximum-Modul ganzer transzendenter Funktionen.

Von I. VINCZE in Budapest.

Einleitung.

1. In der vorliegenden Note beschäftigen wir uns mit der Frage, was man in Kenntnis des Maximum-Moduls $M(r)$ einer ganzen transzendenten Funktion $F(z)$ über die Koeffizienten der Potenzreihe von $F(z)$ aussagen kann. In neuerer Zeit hat W. K. HAYMAN dieses Problem [3] für gewisse ganze Funktionen und auch für Potenzreihen mit endlichem Konvergenzradius ausgearbeitet. Die Bedeutung des Problems wird in seiner Arbeit an zahlreichen Beispielen erläutert; wenn z. B. die Potenzreihe von $F(z)$ nicht bekannt, oder schwer zu behandeln ist, der Maximum-Modul von $F(z)$ sich jedoch bestimmen läßt, so kann man auch für die Koeffizienten der Potenzreihe eine asymptotische Darstellung angeben. Es ist z. B. $e^{P(z)}$ eine solche Funktion, wobei $P(z)$ ein Polynom mit nichtnegativen Koeffizienten bedeutet. — Unsere Arbeit enthält einige mit elementaren Methoden erreichte Sätze in dieser Richtung für *beliebige* ganze Funktionen. Die Resultate können wahrscheinlich noch verschärft werden.

2. Nach der Ungleichung von CAUCHY gilt

$$|a_n| \leqq \frac{M(r)}{r^n}.$$

Gleichheit kann nur im Falle eines Polynoms bestehen, was wir im folgenden außer Acht lassen werden. Es liegt nun an der Hand zu versuchen, aus dieser Ungleichung die schärfste Abschätzung für $|a_n|$ zu finden, also denjenigen Wert von r zu bestimmen, für den $\frac{M(r)}{r^n}$ minimal ist. Dieser Wert ist für jedes n eindeutig bestimmt, was schon durch CAUCHY [2] erwähnt wurde; wir werden ihn mit r_n bezeichnen[1]). Es besteht also die Ungleichung

$$(1) \qquad |a_n| < M_n = \frac{M(r_n)}{r_n^n} = \min_{0<r<\infty} \left\{ \frac{M(r)}{r^n} \right\}.$$

[1]) Mit einigen Eigenschaften des Wertsystems r_n hat sich Verf. [6] beschäftigt.

Wir führen die Funktion

$$n(r)=r\frac{M'(r)}{M(r)}$$

ein; wegen der logarithmischen Konvexität von $M(r)$ ist $n(r)$ monoton zunehmend, sie kann jedoch abzählbar unendlich viele Sprungstellen haben. Wie wir sehen werden, sind die Zahlen r_n durch die Relation $n(r)=n$ $(n=1,2,3,\ldots)$ bestimmt. Daher ist die Zahlenfolge r_n monoton nicht abnehmend und die Zahlen r_n, als Minimumstellen der Funktion $\frac{M(r)}{r^n}$, für jedes *reelle* $n>0$ definiert. Den Zusammenhang zwischen der Wachstumsordnung von $F(z)$ und dem Verhalten von $n(r)$ gilt der in § 1 bewiesene

Satz 1. *Es gilt*[2]) *für* $r\to\infty$

$$\begin{matrix}\limsup\\ \liminf\end{matrix}\frac{\log n(r)}{\log r}=\begin{matrix}\limsup\\ \liminf\end{matrix}\frac{\log\log M(r)}{\log r}.$$

In § 1 werden wir uns mit einigen einfachen Eigenschaften der Folge $r_1, r_2, \ldots$ beschäftigen. In § 2 werden einige einfache Ungleichungen über die Momente

$$\mu_n=\int_0^\infty\frac{r^n}{M(r)}dr$$

sowohl mittels der Werte M_n, als auch mit Hilfe der Koeffizienten der Potenzreihe von $F(z)$ abgeleitet.

3. Während das Maximalglied den Ausdruck $M(r)-|a_n|r^n$ minimisiert, wird in den Punkten r_n die relative Abweichung

$$\frac{M(r)-|a_n|r^n}{M(r)}$$

zum Minimum. Daß sich $M(r)$ mit irgendeinem Glied der Potenzreihe von $F(z)$ am besten in den Punkten r_n abschätzen läßt, wird aus der folgenden Bemerkung klar: zu einem beliebigen r gibt es einen Index n derart, daß die Ungleichung

$$\frac{\mu(r)}{M(r)}\leqq\frac{\mu(r_n)}{M(r_n)}<1$$

gilt, nämlich $n=\nu(r)$. Dies folgt sofort aus der Definition des Maximalglie-

---

[2]) Für den Fall einer Potenzreihe mit positiven Koeffizienten, und nur für die Aussage über lim sup, vgl. Pólya—Szegő, *Aufgaben und Lehrsätze aus der Analysis*, Bd. II (Berlin, 1925), Aufg. 53, S. 8, Lösung S. 178.

des $\mu(r)$ und aus (1):

$$\frac{\mu(r)}{M(r)} = \frac{|a_{\nu(r)}| r^{\nu(r)}}{M(r)} \leqq \frac{|a_{\nu(r)}| r_{\nu(r)}^{\nu(r)}}{M(r_{\nu(r)})} \leqq \frac{|a_k| r_{\nu(r)}^{k}}{M(r_{\nu(r)})} < 1,$$

wobei $k = \nu(r_{\nu(r)})$ ist.

Es sei noch hier erwähnt, daß P. ERDÖS und T. KÓVÁRI [4] zu jeder ganzen Funktion mittels der Punkte r_n eine Potenzreihe $N(r)$ mit positiven Koeffizienten konstruierten, für welche

$$\frac{1}{6} < \frac{M(r)}{N(r)} < 3$$

gilt. Im Zusammenhang mit einem Problem von L. KALMÁR und P. TURÁN haben sie in [4] ein Beispiel für eine ganze Funktion angegeben, deren Maximum-Modul keiner Potenzreihe mit positiven Koeffizienten asymptotisch gleich ist.

Für die Koeffizienten gewisser ganzer Funktionen und auch für die Koeffizienten von Potenzreihen mit endlichem Konvergenzradius hat W. K. HAYMAN [3] die folgende asymptotische Darstellung angegeben:

$$a_n \sim \frac{M_n}{\sqrt{2\pi b(r_n)}} \qquad (n \to \infty), \tag{2}$$

wobei M_n dasselbe bedeutet, wie in (1), und

$$b(r) = \frac{d^2 \log M(r)}{d(\log r)^2}.$$

Wendet man (2) auf die Potenzreihe von e^z an, so erhält man die Stirlingsche Formel; daher kann (2) als eine Verallgemeinerung der Stirlingschen Formel aufgefaßt werden.

Nach (1) ist $\frac{|a_n|}{M_n} < 1$; wir werden zeigen, daß die Folge dieser Quotienten nicht zu rasch gegen Null konvergieren kann.

Satz 2. *Es gilt*

$$\sum_{n=0}^{\infty} \frac{|a_n|}{M_n} = \infty.$$

Hieraus folgt für beliebiges $\varepsilon > 0$ die Existenz unendlich vieler n mit

$$\frac{1}{n^{1+\varepsilon}} < \frac{|a_n|}{M_n}.$$

Nach WIMAN und VALIRON [5] gilt zwar $M(r) < \nu(r)^{\frac{1}{2}+\varepsilon} \mu(r)$ bis auf gewisse Intervalle von r, es ist aber eine offene Frage, wo die Ausnahmestellen liegen.

In Kenntnis von $M(r)$ gibt der folgende Satz eine gewisse Auskunft über die Größe der Lücken, die in der Potenzreihe von $F(z)$ auftreten können:

Satz 3. *Gilt für ein Paar natürlicher Zahlen n, s (mit $s > n$)*

$$\frac{r_s}{r_n} \geqq 5,$$

so gibt es unter den Koeffizienten $a_{n-2}, a_{n-1}, a_n, \ldots, a_s$ mindestens einen, der nicht verschwindet.

4. Im Falle der Funktion $F(z) = e^z = \Sigma a_n z^n$ gilt

$$\frac{1}{a_n} = \int_0^\infty \frac{r^n}{M(r)}\, dr, \quad \text{d.h.} \quad n! = \int_0^\infty r^n e^{-r}\, dr \qquad (n = 1, 2, \ldots).$$

Daß zwischen den Koeffizienten und den erwähnten Momenten ein allgemeinerer Zusammenhang besteht, kann man aus folgenden vermuten:

Bei beliebig klein gegebenem positivem ε gilt für unendlich viele n

$$\frac{1}{|a_n|} < n^{1+\varepsilon} \int_0^\infty \frac{r^n}{M(r)}\, dr.$$

Unter speziellen Voraussetzungen gilt der

Satz 4. *Gilt für irgendeine ganze Funktion* $\limsup_{n\to\infty} \sqrt[n]{r_n} = 1$, *so ist auch*

$$\limsup_{n\to\infty} \left(\int_0^\infty \frac{|a_n| r^n}{M(r)} \right)^{\frac{1}{n}} = 1.$$

§ 1. Über die Folge r_n.

1. Zuerst machen wir einige vorbereitende Bemerkungen.

Nach BLUMENTHAL [1] ist $M(r)$ stückweise analytisch, $M'(r)$ kann jedoch abzählbar unendlich viele Sprungstellen haben ($M'(r+0) \geqq M'(r-0)$). Für die Funktion

$$S_n(r) = \frac{M(r)}{r^n}$$

gilt daher

$$S_n'(r \pm 0) = \frac{M(r)}{r^{n+1}} \left(r \frac{M'(r \pm 0)}{M(r)} - n \right).$$

Nach dem Hadamardschen Dreikreisensatz gilt ferner in jeder Stetig-

keitsstelle von $M'(r)$ und $M''(r)$

$$\frac{d^2 \log M(r)}{d(\log r)^2} = r \frac{d}{dr}\left(r \frac{M'(r)}{M(r)}\right) > 0.$$

Die Funktion $n(r) = rM'(r)/M(r)$ ist also monoton streng zunehmend. Ist die Funktion $F(z)$, wie angenommen, transzendent, so strebt $n(r)$ mit $r \to \infty$ gegen Unendlich und ist bis auf die Sprungstellen analytisch; daher nimmt sie an oder überspringt den Wert $n\,(>0)$ nur an einer einzigen Stelle. Hieraus folgt, daß $S_n(r)$ eine einzige Minimumstelle $r = r(n)$ besitzt. Auf diese Weise ist eine wegen der Monotonität von $n(r)$ ebenfalls monoton wachsende Funktion $r_n = r(n)$ definiert. Sie ist als inverse Funktion von $n(r)$ stetig.

2. Nun wenden wir uns dem Beweis des Satzes 1 zu. Da $n(r)$ die inverse Funktion von r_n ist, folgt aus der Eigenschaft von r_n als Minimumstelle:

$$\frac{M(r)}{r^{n(r)}} \leqq \frac{M(\varrho)}{\varrho^{n(r)}} \qquad (r > 0, \varrho > 0).$$

Ist ϱ festgelegt, so wähle man r so groß, daß

$$M(\varrho) < \left(\frac{r}{\varrho}\right)^{n(r)}$$

gilt. Dann gilt

$$M(r) < \left(\frac{r}{\varrho}\right)^{n(r)} M(\varrho) < \left(\frac{r}{\varrho}\right)^{2n(r)},$$

oder

$$\log M(r) < n(r) \log \left(\frac{r}{\varrho}\right)^2, \quad \frac{\log \log M(r)}{\log r} < \frac{\log n(r) + \log \log \left(\frac{r}{\varrho}\right)^2}{\log r},$$

woraus wegen

$$\frac{\log \log \left(\frac{r}{\varrho}\right)^2}{\log r} \to 0 \quad \text{für} \quad r \to \infty$$

$$\begin{matrix}\limsup \\ \liminf\end{matrix} \frac{\log \log M(r)}{\log r} \leqq \begin{matrix}\limsup \\ \liminf\end{matrix} \frac{\log n(r)}{\log r} \tag{1.1}$$

folgt.

Andererseits gilt

$$\frac{n(r \pm 0)}{r} = \frac{M'(r \pm 0)}{M(r)},$$

also

$$\int_{\varrho}^{r} \frac{n(t)}{t}\, dt = \log M(r) - \log M\left(\frac{r}{e}\right).$$

Ist nun $M\left(\frac{r}{e}\right) > 1$, so gilt wegen der Monotonie von $n(r)$

$$n\left(\frac{r}{e}\right) < \log M(r),$$

also

$$\frac{\log n\left(\frac{r}{e}\right)}{\log \frac{r}{e}} < \frac{\log \log M(r)}{\log r} \frac{1}{1-\frac{1}{\log r}}.$$

Hieraus folgt die zu (1. 1) entgegensetzte Ungleichung. Damit ist unser Satz 1 bewiesen.

3. Es bezeichne wieder M_n das Minimum der Funktion $S_n(r)$, also

$$M_n = \frac{M(r_n)}{r_n^n}.$$

Es gilt für $n \to \infty$

$$0 \leqq \limsup M_n^{\frac{1}{n}} \leqq \lim \frac{M^{\frac{1}{n}}(r)}{r} = \frac{1}{r}$$

für jedes $r > 0$, also ist

$$\lim M_n^{\frac{1}{n}} = 0.$$

Wie bekannt, gilt $\lim |a_n|^{\frac{1}{n}} = 0$. Es besteht jedoch — wie wir es in § 3 sehen werden — für jede ganze, transzendente Funktion

$$\limsup \left(\frac{|a_n|}{M_n}\right)^{\frac{1}{n}} = 1.$$

4. Für die Folgen $\{r_n\}$ bzw. $\{M_n\}$ bestehen folgende einfache Relationen für $n \geqq 1$ und $n \geqq k \geqq 1$:

$$\frac{M_{n-1}}{M_n} \leqq r_n \leqq \frac{M_n}{M_{n+1}} \qquad (M_0 = |F(0)|), \tag{1. 2}$$

$$\frac{r_1}{M(r_1)} \frac{M(r_n)}{r_n} \leqq \frac{r_n^n}{r_1 r_2 \dots r_n} \leqq \frac{M(r_n)}{M(r_1)}, \tag{1. 3}$$

$$r_k^{n-k} \leqq \frac{M_k}{M_n} \leqq r_n^{n-k}. \tag{1. 4}$$

(1. 2) folgt aus der Minimaleigenschaft von r_{n-1} und r_{n+1}:

$$M_{n-1} = \frac{M(r_{n-1})}{r_{n-1}^{n-1}} \leqq \frac{M(r_n)}{r_n^{n-1}} = r_n M_n$$

und

$$M_{n+1} = \frac{M(r_{n+1})}{r_{n+1}^{n+1}} \leqq \frac{M(r_n)}{r_n^{n+1}} = \frac{M_n}{r_n}.$$

(1.3) und (1.4) folgen aus (1.2) durch Multiplikation und aus der Monotonität der Folge r_n.

Für $F(z) = e^z$ erhält man aus (1.2) die wohlbekannte Ungleichung

$$\left(1+\frac{1}{n}\right)^n < e < \left(1+\frac{1}{n}\right)^{n+1}$$

und aus (1.3) die folgende schwächere Gestalt den Stirlingschen Formel:

$$\sqrt[n]{n!} \sim \frac{n}{e}.$$

§ 2. Ungleichungen für gewisse Momente.

In folgendem werden wir die Momente

$$\mu_n = \int_0^\infty \frac{r^n}{M(r)}\, dr$$

mittels der M_n und auch mittels der Koeffizienten der Potenzreihe von oben abschätzen.

Sind a, b, n reell und nichtnegativ, $b < n+1$, so gilt

$$\mu_n < \frac{a+b}{ab} M_{n+1+a}^{-\frac{b}{a+b}} M_{n+1-b}^{-\frac{a}{a+b}}, \tag{2.1}$$

$$\mu_n < \frac{1}{M_n}\left[\frac{a+1}{a}\left(\frac{M_n}{M_{n+1+a}}\right)^{\frac{1}{a+1}} - \frac{b-1}{b}\left(\frac{M_{n-b+1}}{M_n}\right)^{\frac{1}{b-1}}\right]. \tag{2.2}$$

Beweis. Es gilt wegen der Minimaleigenschaft von r_ν $(\nu > 0)$

$$M_\nu = \frac{M(r_\nu)}{r_\nu^\nu} \leqq \frac{M(r)}{r^\nu}, \text{ also } \frac{r^n}{M(r)} \leqq \frac{1}{M_\nu} r^{n-\nu}. \tag{2.3}$$

Setzt man $\nu = n+a+1$ und $\nu = n-b+1$ (>0), so folgt

$$\frac{r^n}{M(r)} \leqq \min\left\{\frac{1}{M_{n+1+a}} r^{-a-1},\ \frac{1}{M_{n+1-b}} r^{b-1}\right\}.$$

Für

$$r = \bar{r} = \left(\frac{M_{n+1-b}}{M_{n+1+a}}\right)^{\frac{1}{a+b}}$$

werden die beiden, zwischen { } stehenden Ausdrücke gleich; für $0<r<\bar{r}$ ist also der zweite, für $\bar{r}<r<\infty$ jedoch der erste Ausdruck der kleinere. Also gilt

$$\mu_n < \frac{1}{M_{n+1-b}} \int_0^{\bar{r}} r^{b-1}\,dr + \frac{1}{M_{n+1+a}} \int_{\bar{r}}^{\infty} \frac{1}{r^{a+1}}\,dr = \frac{1}{M_{n+1-b}} \frac{\bar{r}^b}{b} + \frac{1}{M_{n+1+a}} \frac{\bar{r}^{-a}}{a},$$

woraus nach Einsetzen des Wertes von $\bar{r}$ (2. 1) folgt.

Zum Beweis von (2. 2) bestimme man zuerst die Zahlen $\tilde{r}$ und $\tilde{\tilde{r}}$ derart, daß $\frac{\tilde{r}^{b-1}}{M_{n+1-b}} = \frac{1}{M_n}$ und $\frac{\tilde{\tilde{r}}^{-a-1}}{M_{n+1+a}} = \frac{1}{M_n}$; dann wende man (2. 3) für $\nu = n+1-b$ im Intervall $0<r\leqq\tilde{r}$, für $\nu = n+1+a$ im Intervall $\tilde{\tilde{r}}\leqq r\leqq\infty$, und für $\nu = n$ im Intervall $\tilde{r}<r<\tilde{\tilde{r}}$ an. — Aus (1. 4) folgt, daß $\tilde{r}\leqq\tilde{\tilde{r}}$ immer besteht.

Wegen $|a_n|<M_n$ können wir in (2. 3) $|a_\nu|$ anstatt M_ν setzen, also

$$\frac{r^n}{M(r)} < \frac{1}{|a_\nu|} r^{n-\nu} \tag{2. 3'}$$

schreiben. Mit Hilfe dieser Ungleichung lassen sich auf ähnliche Weise die folgenden Ungleichungen ableiten:

$$\mu_n < \frac{a+b}{ab} |a_{n+a+1}|^{-\frac{b}{a+b}} |a_{n-b+1}|^{-\frac{a}{a+b}}, \tag{2. 1'}$$

$$\mu_n < \frac{1}{|a_n|}\left(\frac{a+1}{a}\left|\frac{a_n}{a_{n+a+1}}\right|^{\frac{1}{a+1}} - \frac{b-1}{b}\left|\frac{a_{n-b+1}}{a_n}\right|^{\frac{1}{b-1}}\right), \tag{2. 2'}$$

für die Gültigkeit von (2. 2') muß man jedoch noch

$$\left|\frac{a_n}{a_{n+a+1}}\right|^{\frac{1}{a+1}} \geqq \left|\frac{a_{n-b+1}}{a_n}\right|^{\frac{1}{b-1}}$$

voraussetzen, damit $\tilde{r}<\tilde{\tilde{r}}$ herausfällt.

Es sei weiterhin eine interessante Folgerung von (2. 1') erwähnt: Ist in der Potenzreihe einer transzendenten Funktion $|a_1| = |a_N| = 1$, so besteht für $n = 2, 3, \ldots, N-2$

$$\mu_n < \frac{N-1}{n(N-1-n)},$$

d. h. es gilt zwar $\mu_n \to \infty$ für $n \to \infty$, jedoch die ersten $N-2$ Glieder der Folge $\mu_1, \mu_2, \ldots$ sind klein.

Setzt man insbesondere

$$F(z)=e^z=1+\frac{z}{1!}+\frac{z^2}{2!}+\cdots,$$

so ist

$$\mu_{N-2}=(N-2)!.$$

Wenn wir aber in dieser Potenzreihe von e^z nur einen Koeffizienten verändern, wenn wir also die Potenzreihe

$$F^*(z)=1+\frac{z}{1!}+\cdots+\frac{z^{N-1}}{(N-1)!}+z^N+\frac{z^{N+1}}{(N+1)!}+\cdots$$

betrachten, so besteht für diese

$$\mu^*_{N-2}<1.$$

§ 3. Sätze über die Koeffizienten.

1. Der in der Einleitung erwähnte Satz 2 ist eine einfache Konsequenz der folgenden, für jedes r und für jedes natürliche n gültigen Relation:

$$1=\frac{M(r)}{M(r)}\leqq\frac{\sum_{k=0}^{\infty}|a_k|r^k}{M(r)}=\frac{\sum_{k=0}^{n-1}|a_k|r^k}{M(r)}+\sum_{k=n}^{\infty}|a_k|\frac{r^k}{M(r)}<$$

$$<\frac{\sum_{k=0}^{n-1}|a_k|r^k}{M(r)}+\sum_{k=n}^{\infty}\frac{|a_k|}{M_k}.$$

Da bei festgelegtem n die Relation

$$\lim_{r\to\infty}\frac{\sum_{k=0}^{n-1}|a_k|r^k}{M(r)}=0$$

gilt, so ist für jedes n

$$\sum_{k=n}^{\infty}\frac{|a_k|}{M_k}\geqq 1,$$

woraus Satz 2 der Einleitung schon folgt.

2. Zum Beweis des Satzes 3 betrachte man zu einem gegeben Index n einen weiteren Index s, so daß $s>n$ und $r_s>r_n$ gilt. Es seien ferner r und r' zwei Zahlen mit

$$r_n<r<r'<r_s.$$

Bezeichnet man nun $\mathfrak{M}(\varrho)=\sum_0^\infty |a_k|\varrho^k$, so gilt wegen $M(\varrho)\leqq\mathfrak{M}(\varrho)$

$$1=\frac{1}{r'-r}\int_r^{r'} d\varrho \leqq \frac{1}{r'-r}\int_r^{r'}\frac{\mathfrak{M}(\varrho)}{M(\varrho)}\,d\varrho=\frac{1}{r'-r}\int_r^{r'}\frac{\sum_0^\infty |a_k|\varrho^k}{M(\varrho)}\,d\varrho=$$

$$(3.1)\qquad =\frac{1}{r'-r}\sum_0^{n-3}|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho+\frac{1}{r'-r}\sum_{n-2}^{s}|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho+$$

$$+\frac{1}{r'-r}\sum_{s+1}^{\infty}|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho.$$

Wir schätzen jetzt die ersten und dritten Summen ab. Es gilt für $k\leqq n-3$

$$(3.2)\qquad \frac{|a_k|\varrho^k}{M(\varrho)}=\frac{|a_k|\varrho^n}{M(\varrho)}\frac{1}{\varrho^{n-k}}\leqq\frac{|a_k|}{M_n}\frac{1}{\varrho_{n-k}}=\frac{|a_k|}{M_k}\frac{M_k}{M_n}\frac{1}{\varrho_r^{n-k}}<\left(\frac{r_n}{\varrho}\right)^{n-k}.$$

Es ist nämlich $\frac{|a_k|}{M_k}<1$ und nach (1.4) des § 1 $\frac{M_k}{M_n}<r_n^{n-k}$. Daher ist

$$|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho\leqq\int_r^{r'}\left(\frac{r_n}{\varrho}\right)^{n-k}d\varrho=\frac{r_n^{n-k}}{n-k-1}\left(\frac{1}{r^{n-k-1}}-\frac{1}{r'^{n-k-1}}\right),$$

also

$$\frac{1}{r'-r}\sum_0^{n-3}|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho\leqq\sum_{k=0}^{n-3}\frac{1}{n-k-1}\frac{r_n}{r'-r}\left[\left(\frac{r_n}{r}\right)^{n-k-1}-\right.$$

$$\left.-\left(\frac{r_n}{r'}\right)^{n-k-1}\right]\leqq\sum_{k=2}^{\infty}\frac{1}{k}\frac{r_n}{r'-r}\left[\left(\frac{r_n}{r}\right)^k-\left(\frac{r_n}{r'}\right)^k\right].$$

Gilt nun $k\geqq s+1$, so erhalten wir genau wie (3.2) die Ungleichung

$$\frac{|a_k|\varrho^k}{M(\varrho)}<\left(\frac{\varrho}{r_s}\right)^{k-s}.$$

Daher ist

$$|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho\leqq\frac{1}{k-s+1}\frac{1}{r_s^{k-s}}(r'^{k-s+1}-r^{k-s+1})$$

und

$$\frac{1}{r'-r}\sum_{k=s+1}^{\infty}|a_k|\int_0^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho<\sum_{k=2}^{\infty}\frac{1}{k}\frac{r_s}{r'-r}\left[\left(\frac{r'}{r_s}\right)^k-\left(\frac{r}{r^s}\right)^k\right].$$

Aus (3. 1) erhalten wir nun

$$1 \leqq \frac{1}{r'-r}\sum_{n=2}^{s}|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho+\frac{r_n}{r'-r}\sum_{k=2}^{\infty}\frac{1}{k}\left[\left(\frac{r_n}{r}\right)^k-\left(\frac{r_n}{r'}\right)^k\right]+$$

$$+\frac{r_s}{r'-r}\sum_{k=2}^{\infty}\frac{1}{k}\left[\left(\frac{r'}{r_s}\right)^k-\left(\frac{r}{r_s}\right)^k\right].$$

Man setze nun $\frac{r}{r_n}=x$, $\frac{r'}{r_n}=y$, $\frac{r_s}{r_n}=a$ $(1<x<y<a)$, dann gilt

$$1<\frac{1}{r'-r}\sum_{n=2}^{s}|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho+\frac{1}{y-x}\sum_{k=2}^{\infty}\frac{1}{k}\left(\frac{1}{x^k}-\frac{1}{y^k}\right)+$$

$$+\frac{a}{y-x}\sum_{k=2}^{\infty}\frac{1}{k}\left[\left(\frac{y}{a}\right)^k-\left(\frac{x}{a}\right)^k\right].$$

Aus der für $0 \leqq u < 1$ gültigen Potenzreihe der Funktion $\log\frac{1}{1-u}$ ergibt sich

$$1<\frac{1}{r'-r}\sum_{n=2}^{s}|a_k|\int_r^{r'}\frac{\varrho^k}{M(\varrho)}\,d\varrho+\frac{1}{y-x}\log\left[\frac{y-1}{x-1}\,\frac{x}{y}\left(\frac{a-x}{a-y}\right)^a\right]-1-\frac{1}{yx}.$$

Wenn wir nun die Werte von x und y so wählen können, daß

$$\frac{1}{y-x}\log\left[\frac{y-1}{x-1}\,\frac{x}{y}\left(\frac{a-x}{a-y}\right)^a\right]-1-\frac{1}{xy}<1 \tag{3. 3}$$

besteht, so muß $\sum_{n=2}^{s}\frac{|a_k|}{M_k}>0$ sein; damit wird auch unser Satz bewiesen sein. Nun läßt sich (3. 3) auf die folgende Gestalt bringen:

$$f_n(x)=\frac{x(a-x)^a}{x-1}e^{2x-\frac{1}{x}}<\frac{y(a-y)^a}{y-1}e^{2y-\frac{1}{y}}=f_n(y).$$

Die Existenz eines Punktpaars x, y $(1<x<y<a)$ mit dieser Eigenschaft folgt nun für $a \geqq 5$ (und ja sogar für $a>14/3$) daraus, daß, wie man leicht nachrechnet, $f_n'(2)$ für diese Werte von a *positiv* ausfällt.

3. Nun beweisen wir unseren Satz 4. Aus (2. 2) des § 2 und aus (1. 4) des § 1 folgt

$$\int_0^{\infty}\frac{|a_n|r^n}{M(r)}\,dr<\frac{|a_n|}{a}\,\frac{a+1}{M_n}\left(\frac{M_n}{M_{n+a+1}}\right)^{\frac{1}{n+1}} \leqq \frac{|a_n|}{M_n}\,\frac{a+1}{a}\,r_{n+a+1}.$$

Da für $n \to \infty$ voraussetzungsgemäß

$$\limsup \sqrt[n]{r_{n+\sigma+1}} = \limsup \left(\sqrt[n+\sigma+1]{r_{n+\sigma+1}} \right)^{1+\frac{\sigma+1}{n}} = 1$$

ist, so besteht

$$\limsup \left(\int_0^\infty \frac{|a_n| r^n}{M(r)} dr \right)^{\frac{1}{n}} \leqq 1.$$

Andererseits gilt

$$1 \leqq \frac{\mathfrak{M}(r)}{M(r)} = \sum_0^\infty |a_k| \frac{r^k}{M(r)}$$

oder, indem man von R bis $R+1$ integriert,

$$1 \leqq \sum_0^\infty |a_k| \int_R^{R+1} \frac{r^k}{M(r)} dr < \sum_0^n |a_k| \int_R^{R+1} \frac{r^k}{M(r)} dr + \sum_{n+1}^\infty |a_k| \int_0^\infty \frac{r^k}{M(r)} dr,$$

was für jedes feste n gültig ist. Strebt nun R gegen Unendlich, so gilt

$$\sum_{k=0}^n \int_R^{R+1} |a_k| \frac{r^k}{M(r)} dr \to 0,$$

woraus die Divergenz der Reihe $\sum_0^\infty \int_0^\infty \frac{|a_k| r^k}{M(r)} dr$ folgt. Daraus ergibt sich

$$\limsup_{n \to \infty} \left(\int_0^\infty \frac{|a_n| r^n}{M(r)} dr \right)^{\frac{1}{n}} \geqq 1, \tag{3.4}$$

womit Satz 4 bewiesen ist.

Aus der Divergenz der Reihe $\sum_0^\infty a_n \mu_n$ folgt weiterhin unsere in der Einleitung zu Satz 4 gestellte Bemerkung.

Literatur.

[1] O. Blumenthal. Sur le mode de croissance des fonctions entières, *Bull. Soc. Math. France*, **35** (1907), 213—32.
[2] A. Cauchy, *Oeuvres complètes*, Bd. 9 (Paris, 1896), 75.
[3] W. K. Hayman, A Generalisation of Stirling's Formula, *Journal für die reine und angew. Math.*, **196** (1956), 67—95.
[4] P. Erdős—T. Kővári, On the maximum modulus of entire functions, *Acta Math. Hung.*, 7 (1957), 305—318.
[5] G. Valiron, *Lectures on the general theory of integral functions* (Toulouse, 1923), 106.
[6] I. Vincze, Transzcendens egész függvények maximum modulusáról, *Magyar Tud. Akad. III. Oszt. Közl.*, **6** (1956), 451—459.

(Eingegangen am 22. September 1957.)

Bibliographie.

Marc Zamansky, La sommation des séries divergentes (Mémorial des Sciences Mathématiques, fascicule CXXVIII), 46 pages, Paris, Gauthier-Villars, 1954.

Les procédés appliqués à la sommation des séries divergentes, les résultats et les méthodes de démonstration utilisées dans la théorie de la sommation sont diverses et multiples. Le but de l'auteur est de servir d'un fil conducteur dans l'étude de cette théorie. Dans l'introduction sont énumérés, sans faire mention des applications, les procédés linéaires les plus connus (les procédés restreints de NÖRLUND, CESÀRO, HÖLDER, RIESZ, HAUSDORFF, et les procédés complets d'ABEL, RIEMANN, LAMBERT et BOREL) et sont exposés les problèmes de la régularité et de l'inclusion des procédés de sommation. La première partie contient les résultats connus les plus importants concernant les problèmes de la régularité et de l'inclusion des procédés restreints usuels. La deuxième partie est consacrée aux procédés de sommation engendrés par une fonction sommatoire. Tel procédé est défini de la façon suivante. Soit $g(t)$ une fonction réelle, continue et à variation bornée pour $0 \leqq t \leqq 1$, telle que $g(0) = 1$. Si pour $x \to \infty$ la somme $\sum_{0 \leqq k \leqq x} g\left(\frac{k}{x}\right) u_k$ a une limite finie S, on dit que $\sum_{k=0}^{\infty} u_k$ est sommable et a pour somme S. Les résultats propres de l'auteur se rattachant aux problèmes de la régularité et de l'inclusion de tels procédés sont mentionnés sans démonstration. La méthode employée repose sur l'application des transformées de Mellin et de Laplace de la fonction sommatoire. La même méthode fournit des résultats intéressants aussi pour les procédés linéaires usuels. La troisième partie signale quelques résultats concernant les procédés complets. Enfin, on trouve des Notes dont le but est d'indiquer quelques généralisations, de montrer que les théorèmes taubériens de Wiener peuvent être présentés par cette méthode, et de suggérer de nouveaux champs d'application.

K. Tandori (Szeged)

Horst von Sanden, Praxis der Differentialgleichungen, Vierte, erweiterte Auflage. 114 S., Berlin, Walter de Gruyter & Co., 1955.

Dieses bewährte Lehrbuch stellt die praktischen Anwendungen in den Vordergrund, betont die numerischen Lösungsmethoden und beabsichtigt dem Leser eine gewisse Rechenangewandheit zu geben. Statt einer systematischen und exakten Behandlung der Differentialgleichungen gibt der Verfasser einen elementaren und kurzen Überblick über die Theorie der gewöhnlichen, linearen Differentialgleichungen und Differentialgleichungssysteme erster und zweiter Ordnung und der Randwertprobleme. Die verschiedenen Lösungsmethoden werden durch zeichnerische Integration, numerisch angeführte Beispiele erläutert. Gegenüber der dritten Auflage des Buches ist ein neuer Abschnitt über Differenzengleichungen aufgenommen.

K. Tandori (Szeged)

Francesco G. Tricomi, Vorlesungen über Orthogonalreihen (Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen, Band LXXVI), VI + 264 Seiten, Berlin—Göttingen—Heidelberg, Springer Verlag, 1955.

Das Hauptziel des Buches besteht darin, den Leser möglichst rasch in die Theorie der trigonometrischen Reihen und der orthogonalen Polynome einzuführen.

In Kapitel I werden die Elemente der allgemeinen Theorie der orthogonalen Funktionensysteme behandelt, wie z. B. die Abzählbarkeit eines orthogonalen Funktionensystems, der Satz von Riesz—Fischer, Bedingungen für die Vollständigkeit eines Funktionensystems, Vollständigkeit des Systems der trigonometrischen Funktionen und der Potenzen von x, die Parsevalsche Gleichung usw.

Kapitel II—III beschäftigen sich mit den Grundlagen der Theorie der trigonometrischen, insbesondere der Fourierschen Reihen.

Die folgenden Kapitel (IV—VI) sind den Orthogonalpolynomen gewidmet. Während in dem Teil über trigonometrische Reihen das Hauptinteresse auf der Konvergenzfrage liegt, sind in dem Teil über Orthogonalpolynome mehr die individuellen Eigenschaften derselben in den Vordergrund gestellt. Die einheitliche Behandlung der klassischen Orthogonalpolynome beruht auf einer verallgemeinerten Rodriguez-Formel. Diese Formel wird in Kapitel IV bewiesen, hier werden auch andere allgemeinen Eigenschaften der orthogonalen Polynome dargestellt, wie die Rekursionsformel, die Summationsformel von Christoffel—Darboux, Differentialgleichung der klassischen orthogonalen Polynome, Verhalten bei Änderung der Belegungsfunktion, sowie Lage der Nullstellen.

Kapitel V ist den Orthogonalpolynomen in einem endlichen Grundintervall gewidmet. Nach der Behandlung der hypergeometrischen Funktion folgt eine eingehende Diskussion der Jacobischen Polynome; so werden Rekursionsformel, Differentialgleichung, asymptotischer Ausdruck, erzeugende Funktion für die Jacobischen Polynome, Zusammenhang mit der hypergeometrischen Funktion und die Untersuchung der Nullstellen erörtert. Nachher ergeben sich die ähnlichen Ergebnisse für die übrigen Orthogonalpolynome im Wesentlichen als Spezialfälle. Zwei Paragraphen behandeln Kugelfunktionen mit ganzen bzw. beliebigen Indizes.

Kapitel VI behandelt orthogonale Polynome mit unendlichem Grundintervall, insbesondere die Laguerreschen und die Hermiteschen Polynome. Die Untersuchung der Hermiteschen Polynome wird auf die der Laguerreschen Polynome durch gewisse von Szegö stammende Formeln zurückgeführt.

Vom Leser werden als Vorkenntnisse die Grundtatsachen der Differential- und Integralrechnung verlangt. Das klar geschriebene Buch eignet sich auch zum Selbststudium.

T. Szerényi (Szeged)

Carlo Miranda, Equazioni alle derivate parziali di tipo ellittico (Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 2), VIII + 222 Seiten, Berlin—Göttingen—Heidelberg, Springer-Verlag, 1955.

Es gibt manche Handbücher, die die elliptischen partiellen Differentialgleichungen von einem mehr oder minder praktischen Standpunkt aus behandeln. In den vollständigeren findet man auch, wie man die bezüglichen Randwertaufgaben in Integralgleichungen umformen kann und der Studierende oder der Fachmann kann dann weiter in der Literatur der Integralgleichungen nachsuchen. Endlich wird er sogar an anknüpfende Sätze der Funktionalanalysis stossen. Sind ihm aber die Folgerungen wichtig, welche man aus diesen Resul-

taten der Integralgleichungen und der Funktionalanalysis in der Theorie der elliptischen Differentialgleichungen ziehen kann, so findet er meistens ziemlich wenige Unterstützung.

Der Hauptverdienst dieses Buches besteht eben darin, daß es nicht bei diesen Resultaten der Theorie der Integralgleichungen und der Funktionalanalysis stehen bleibt, sondern in knapper Form eine Reihe von Resultaten mit Literaturangaben zusammenstellt, welche sich direkt auf die Theorie der elliptischen Differentialgleichungen beziehen. Es werden dabei neben den Sätzen über Integralgleichungen auch z. B. der Fixpunktsatz von LERAY—SCHAUDER berücksichtigt. In jedem Satze bezüglich Randwertaufgaben werden die Bedingungen sowohl über die Randkurve, als auch über die Randfunktion mit Sorgfalt und Strenge formuliert. Die Literaturangaben am Ende des Werkes erfüllen 28 Seiten. Inhaltsverzeichnis: I. Randwertprobleme für lineare Gleichungen. II. In Integralform dargestellte Funktionen. III. Umformung der Randwertprobleme in Integralgleichungen. IV. Verallgemeinerte Lösungen der Randwertprobleme. V. Direkte Majorierung der Lösungen des Dirichletschen Problems. VI. Nichtlineare Gleichungen. VII. Andere Untersuchungen über elliptische Gleichungen. Gleichungen höheren Grades. Gleichungssysteme.

Géza Freud (Budapest)

H. Dölp—E. Netto, Grundzüge und Aufgaben der Differential- und Integralrechnung nebst den Resultaten, 22-te, verbesserte Auflage, 201 S., Berlin, Verlag Alfred Töpelmann, 1955.

Die Aufgabensammlung von DÖLP—NETTO ist seit Generationen ein vielgebrauchtes Lehrbuch der elementaren Praxis der Differential- und Integralrechnung. Die vorliegende, verbesserte, schön ausgestattete 22-te Auflage wird gewiß die Popularität des Buches noch erweitern.

Béla Sz.-Nagy (Szeged)

W. H. Gottschalk and G. A. Hedlund, Topological Dynamics (American Mathematical Society, Colloquium Publications, vol. XXXVI), VII + 151 p., Providence, R. I., American Math. Society, 1955.

Es Sei T eine topologische Gruppe von Automorphismen eines topologischen Raumes X; $X \times T$ sei durch φ stetig in X abgebildet, derart, daß $\varphi(x, 1) = x$, $\varphi(x, st) = \varphi(\varphi(x, t), s)$ (x in X; s, t in T) gilt. Dies ist eine Verallgemeinerung folgender klassischen Situation: X ist der Phasenraum eines Systems von endlichvielen Massenpunkten bzw. eine invariante Fläche in demselben; die Hamilton-Funktion hängt nicht explizit von der Zeit ab; T ist die der Phasenströmung entsprechende einparametrige Gruppe, $Tx = (tx = \varphi(x, t) \mid t \text{ in } T)$ also die Bahn des Phasenpunktes; man untersucht Wiederkehr-, Mittelwert- und Mischungseigenschaften dieser Strömung; hinsichtlich der Methode bestehen dabei mehrere Möglichkeiten; man kann a) mit dem (nach LIOUVILLE vorhandenen) T-invarianten Maß m arbeiten (vgl. E. HOPF, *Ergodentheorie*, Berlin 1937), b) sich auf rein topologische Untersuchungen beschränken oder c) maßtheoretische Begriffsbildungen mit topologischen kombinieren (vgl. OXTOBY, Ergodic sets, *Bull. Amer. Math. Soc.*, **58** (1952)). Untersuchungen vom Typ b) liegen bereits bei G. D. BIRKHOFF (*Dynamical Systems*, Amer. Math. Soc. Coll. Publ. IX, 1927) vor.

Im ersten Teil der vorliegenden — ebenfalls zum Typ b) zählenden — Monographie werden diese Untersuchungen auf jede erdenkliche Weise verallgemeinert und systematisiert. Es erscheinen zahlreiche Wiederkehrbegriffe, sowie Sätze, die das Vorkommen und die gegenseitige Abhängigkeit dieser Begriffe zum Inhalt haben. Beispielsweise wird der

Begriff der Periodizität wie folgt verallgemeinert: Sei x in X, dann heißt $P=(t \mid tx=x)$ die Periode von x; eine Menge M in T heißt syndetisch, wenn es eine kompakte Menge K in T mit $KT=T$ gibt. Ist die Periode P von x syndetisch, so heißt x periodisch. Ist für jede Umgebung U von x die Menge $(t \mid tx$ in $U)$ syndetisch, so heißt x fastperiodisch. Ist X kompakt, so gibt es minimal-invariante abgeschlossene Mengen M in X; sie bestehen dann aus fastperiodischen Punkten (dabei darf man in T sogar die diskrete Topologie nehmen: K wird endlich). Es erscheinen einige bekannte Sätze, wie z. B. der Mittelwertsatz für die klassischen fastperiodischen Funktionen.

Im zweiten Teil des Buches werden spezielle Beispiele (die symbolische Dynamik von Morse–Hedlund, die geodätische Strömung auf Flächen konstanter negativer Krümmung, Zylinderströmungen; T ist hier stets zyklisch bzw. einparametrig) auf das Vorkommen dieser Begriffe untersucht. Dabei treten Sätze auf, die man in wesentlich schärferer Form als Sätze von Typus a) kennt, so z. B. der Satz von der Transitivität der erwähnten geodätischen Strömungen; die Abschwächung ist durch den Verzicht auf das (in natürlicher Weise gegebene) invariante Maß m bedingt.

Das Buch ist im Landau-Stil geschrieben und nur dann leicht zu lesen, wenn man es ganz liest. Es empfiehlt sich, bei der Lektüre stets an den oben erwähnten klassischen Spezialfall zu denken. Die außerordentliche systematische und organisatorische Leistung der Verfasser dürfte vor allem dem Spezialisten zugute kommen.

K. Jacobs (München)

Wilhelm Specht, Gruppentheorie (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Band LXXXII), VIII + 457 Seiten, Berlin—Göttingen—Heidelberg, Springer-Verlag, 1956.

Dieses großangelegte Buch enthält in ihren Hauptzügen die Theorie der abstrakten Gruppen. Das Hauptgewicht fällt auf die Gruppen von beliebiger Mächtigkeit, jedoch finden erfreulicherweise auch die endlichen Gruppen vielmals eine besondere Beachtung.

Das Buch gliedert sich in drei fast gleich große Teile mit den Überschriften: 1. Einführung; 2. Freie und direkte Zerlegung; 3. Allgemeine Strukturtheorie. Die Teile umfassen insgesamt elf Kapitel: 1.1. Grundlagen; 1.2. Die Untergruppen einer Gruppe; 1.3. Homomorphie und Isomorphie; 1.4. Gruppen mit Operatoren; 2.1. Die freien Gruppen; 2.2. Freie Zerlegungen; 2.3. Direkte Zerlegung; 2.4. Theorie der abelschen Gruppen; 3.1. Theorie der Normalfolgen; 3.2. Theorie der p-Gruppen; 3.3. Erweiterungstheorie. Die Kapitel selbst sind dann noch in Abschnitte geteilt.

Der Zweck des Verfassers ist der systematische Aufbau des Lehrstoffes. Dabei wird in dem Sinne Vollständigkeit erstrebt, daß der Leser in den behandelten einzelnen Problemkreisen mit den bis heute erreichten äußersten Forschungsresultaten bekannt gemacht wird. Wo das durch den ohnehin großen Umfang des Buches nicht ermöglicht war, leiten den Leser die am Ende des Buches stehenden wertvollen (literarischen) Bemerkungen und Hinweise in die Wege. Aus dem Riesenmaterial des Buches werde die im letzten Kapitel betrachtete, recht schwierige Erweiterungstheorie von Baer hervorgehoben, die zum erstenmale in einem Lehrbuch Platz fand. Auch wurden viele Resultate der sowjetischen Gruppentheoretiker aufgenommen. Jedoch konnten die Betrachtungen nicht auf alle wichtigen Forschungsgebiete der Gruppentheorie erstreckt werden. So wurde insbesondere die Darstellungstheorie beseitigt, auch fanden Anwendungen der Gruppentheorie keinen Platz.

Ein wirksames Hilfsmittel der erzielten Systematisierung bildet die in den letzten drei Abschnitten des ersten Teils entwickelte Theorie der abstrakten Gruppeneigenschaften

(für Gruppen mit Operatoren). Im allgemeinen werde unter einer $\mathfrak{e}$-Gruppe eine Gruppe von der Eigenschaft $\mathfrak{e}$ verstanden. Letztere wird eine abstrakte Gruppeneigenschaft genannt, wenn mit einer $\mathfrak{e}$-Gruppe zusammen die mit ihr isomorphen Gruppen ebenfalls $\mathfrak{e}$-Gruppen sind. Verfasser bemerkt, daß die meisten Untersuchungen über Gruppen darin bestehen, daß man bestrebt ist: für passende abstrakte Gruppeneigenschaften $\mathfrak{e}$ die $\mathfrak{e}$-Gruppen mit dem Ziel zu erforschen, auf diesem Wege schließlich alle Gruppen zu beschreiben. Eine fundamentale Rolle spielen die durch die folgenden sechs Forderungen definierten Gruppeneigenschaften: I. Die Einsgruppe ist $\mathfrak{e}$-Gruppe. II. Die Untergruppen von $\mathfrak{e}$-Gruppen sind $\mathfrak{e}$-Gruppen. III. Die homomorphen Bilder von $\mathfrak{e}$-Gruppen sind $\mathfrak{e}$-Gruppen. IV. Eine Gruppe ist eine $\mathfrak{e}$-Gruppe, stets wenn sie einen Normalteiler hat derart, daß dieser und seine Faktorgruppe $\mathfrak{e}$-Gruppen sind. V. Die Vereinigung einer $\mathfrak{e}$-Untergruppenkette ist eine $\mathfrak{e}$-Gruppe. VI. Das Kompositum von zwei $\mathfrak{e}$-Untergruppen ist eine $\mathfrak{e}$-Gruppe. Ferner werden II und V zu II* bzw. V* abgeschwächt, so daß man nur auf normale Untergruppen achtet. Ähnlich entstehen aus VI zwei Abschwächungen VI*, VI**, indem man von einer oder beiden der betrachteten Untergruppen Normalität verlangt. Vor allem beziehen sich auf diese insgesamt zehn „fundamentalen" $\mathfrak{e}$ viele Sätze, zum Beispiel: Aus III und IV folgt VI*; aus I, V*, VI** folgt, daß jede $\mathfrak{e}$-Gruppe genau einen maximalen $\mathfrak{e}$-Normalteiler hat. Man bemerke, daß die Eigenschaft „endlich zu sein" den Forderungen I bis IV genügt. Als Syloweigenschaft $\mathfrak{s}$ wird die Erfülltheit von I bis V definiert. Hierfür gelten den Sylowschen ähnliche Sätze, wobei die maximalen $\mathfrak{s}$-Untergruppen als die $\mathfrak{s}$-Sylowgruppen definiert sind. Viele weitere teils bekannte (abstrakte) Gruppeneigenschaften (darunter mehrere Spezialfälle von $\mathfrak{s}$) werden im Laufe der Betrachtungen untersucht, die ebenfalls einige von I bis VI** erfüllen. Es werde der folgende merkwürdige „Dualitätssatz" extra erwähnt: Im Fall einer abstrakten Gruppeneigenschaft $\mathfrak{e}$ mit I, II*, III, IV bilden in jeder Gruppe die $\mathfrak{e}$-Normalteiler bzw. die Normalteiler mit $\mathfrak{e}$-Faktorgruppe einen nach unten bzw. nach oben abgeschlossenen Verband.

Der Stil des Buches ist sehr knapp, wodurch jedoch die Klarheit nicht gefährdet wird.

Der Verf. rechnet mit der Routine des Lesers im abstrakten Denken, versäumt jedoch nicht, wo es ihm nötig erscheint, die führenden Ideen der Betrachtungen mit wertvollen Bemerkungen hervorzuheben. So zum Beispiel wird klar gemacht, daß die Untersuchung der abelschen Gruppen (ohne Operatoren) hauptsächlich auf den Endomorphismen $A \to A^n$ $(n = 1, 2, \ldots)$ dieser Gruppen beruht. Dagegen ist ohne besondere Bemerkung klar, daß der ganze dritte Teil im wesentlichen die Untersuchung der (ab- und aufsteigenden) Normalfolgen, insbesondere Normalreihen bedeutet.

Beispiele wurden verhältnismäßig wenige aufgenommen und bilden teils einen organischen Bestandteil der Entwicklungen. Obwohl daran an sich nichts auszusetzen ist, ist jedoch beanstandbar, daß die freien Gruppen durch das recht schwierige Beispiel 5 (auf S. 20—21) eingeführt werden.

Im Fall einer Neuauflage wäre es wünschenswert das Buch mit mehreren Beispielen, ferner auch mit Aufgaben zu versehen. Die in den „Bemerkungen und Hinweisen" angeführten vielen literarischen Angaben möchten zu einem „Literaturverzeichnis" ergänzt werden. Es wirkt etwas störend, daß die Definitionen verschiedenartig gefaßt sind. Viele (die wichtigeren) sind den Lehrsätzen ähnlich formuliert und mit ihrem ganzen Text kursiv gedruckt, was teils zu Mißverständnissen Anlaß gibt, teils überflüssig ist. Bei anderen Definitionen werden nur die neu eingeführten Benennungen kursiv gedruckt, was ja dem allgemeinen Brauch mehr entspricht. Eine dritte Art des Definierens geschieht auf S. 92, wo der Kern einer Gruppe im Satz 26 definiert wird. Es ist überhaupt empfehlenswert, daß man auf die althergebrauchte Weise durch „A heißt B" (oder dergleichen) statt „A ist B"

definiert. Die ersten zwei Abschnitte der „Bemerkungen und Hinweise" sollten etwa im Vorwort, aber jedenfalls vorne im Buche Platz finden. Unter den im Buch ohne Beweis mitgeteilten klassischen Sätzen der Gruppentheorie dürfte auch der berühmte Satz von FROBENIUS über die endlichen Gruppen erwähnt werden, der zugleich ein interessantes Beispiel für die Retrakte bildet.

Es kann nicht genügend betont werden, daß dieses Werk eine hervorragende Leistung des ausgezeichneten Verf. ist und gewiß zur wahren Freude der Fachleute und Studierenden dienen wird.

L. Rédei (Szeged)

Nathan Jacobson, Structure of rings (American Mathematical Society, Colloquium Publications, Vol. XXXVII), VII + 263 p., Providence, R. I., American Mathematical Society, 1956.

After having published the two volumes of his "Lectures in abstract algebra" N. JACOBSON has again enriched the algebraic literature with an excellent book.

Since the publication of the author's "Theory of rings" and ARTIN—NESBITT—THRALL'S "Rings with minimum condition", the structure of (associative but not necessary commutative) rings without finiteness assumptions have been discussed by many authors in the last fifteen years. JACOBSON'S brilliant book, written in a clear but rather terse style, gives an excellent study of the most important investigations of the ring theory without finiteness conditions and is a great help for its further development.

The brief summary of this book is as follows.

In Chapter I are introduced the basic concepts of the irreducible module, primitive ring, semi-simple ring and the Perlis—Jacobson radical approached from the point of view of representation. In Chapter II the density theorem for irreducible modules is formulated firstly in the algebraic way, then its topological formulation is given. With the aid of the results arrived at in the first two chapters, the principal theorems on the structure and representation of semi-simple rings satisfying the minimum condition for right ideals are discussed in Chapter III. The theory of idempotent elements and matrix units in arbitrary rings is required for the theory of non-semi-simple rings with minimum conditions. Chapter IV deals with the completely reducible modules which play an important role in the study of primitive rings having minimal one-sided ideals. The main structure theorem characterizes these rings as certain rings of continuous linear transformations. Chapter V is devoted to the properties of Kronecker products of modules and algebras, and the structure of Kronecker products of algebras of known structure is investigated. Completely reducible modules and their centralizers, and the Galois theory for rings of linear transformations are discussed in Chapter VI. The aim of Chapter VII is to lay the foundation for a general theory of division rings. As tools, some of the results considered previously are developed again reducing them to this case. The discussion of the finite and the infinite outer Galois theory for division rings, furthermore the generalizations of WEDDERBURN'S theorem on finite division rings and the CARTAN—BRAUER—HUA theorem are treated. Nil ideals and prime ideals are found in Chapter VIII. The main results about the lower nil radical of BAER and the nil radical defined by LEVITZKI are studied here. In Chapter IX a certain topological space (whose points are the primitive ideals of a ring) called the structure space of the ring is introduced to study the structure of certain classes of rings, namely I-rings, π-regular rings and biregular rings. In the last chapter some applications of the structure theory are taken up. Firstly certain commutativity theorems are discussed, which may be considered as generalizations of WEDDENBURN'S theorem mentioned above. Then

follows the theory of algebras satisfying polynomial identities (*PI*-algebras). The last part of this chapter deals with some problems on algebraic algebras and among others KAPLANSKY's solution of KUROSH's problem is given.

The value of the book is rather increased by the raising of unsolved problems and by the complete bibliography since about 1943. (The earlier references can be found in the bibliography of the author's "Theory of rings".)

J. Szendrei (Szeged)

C. G. J. Jacobi, Canon Arithmeticus. Nach Berechnungen von W. Patz in verbesserter und erweiterter Form neu herausgegeben von H. Brandt (Mathematische Lehrbücher und Monographien, II. Abt., Band II), XVI + 432 S., Berlin, Akademie-Verlag, 1956.

Dieses Tabellenwerk gibt in fast aller Hinsicht mehr und ist Vollständiger, als sein klassischer Vorläufer aus 1839; so trägt es den alten Titel gewiß nur aus Pietät und auf Grund des Erbrechtes der Deutschen Akademie der Wissenschaften zu Berlin. Nur die obere Schranke des Moduls und in einigen Fällen der zugrunde gelegte primitive Wurzel wurden von den Tafeln von JACOBI unverändert übernommen.

Das Werk enthält Index- und Numerustafeln für alle Moduln unter 1000, für die es primitive Wurzeln gibt, außerdem für 2^n mit $n = 4, 5, \ldots, 11$. Die Moduln $2P_0$ mit ungeradem P_0 wurden neu aufgenommen. Für die primitiven Wurzeln g wurden konsequent immer die kleinsten positiven Werte gewählt. Für die ungeraden Primzahlmoduln findet man im Prinzip neue Tabellen, die $\operatorname{ind}(x+1)$ und $\operatorname{ind}(x-1)$ für $\operatorname{ind} x$ geben, also den Additions- und Subtraktionslogarithmen entsprechen. — Der Herausgeber berichtet über die Berechnung der Tabellen und gibt für die Anwendung 24 Beispiele.

Die neuen Tafeln von PATZ und BRANDT werden gewiß für die Forschung gute Hil f leisten.

T. Bakos (Szeged)

A. Delesalle, Carrés magiques, 70 pages, Paris, Gauthier-Villars, 1956.

C'est un livre de caractère intermédiaire entre un traité et un livre de mathématiques amusantes.

La première partie explique des procédés connus pour obtenir des carrés magiques d'ordre n composés des nombres $1, 2, 3, \ldots, n^2$; notamment si l'ordre est un premier > 2, ou un nombre impair, ou pair, suivant les cas. Par la nature même du problème le procédé donné pour n pair est le plus laborieux.

La deuxième partie considère les carrés magiques d'ordre n composés de nombres quelconques (c'est-à-dire que les nombres du carré magique ne sont pas préscrits; pourtant si n n'est pas premier ils doivent vérifier quelques conditions).

La troisième partie énonce des conditions pour des ensembles de nombres capables d'être disposés en carrés magiques.

T. Bakos (Szeged)

Salvatore Cherubino, Calcolo delle matrici (Consiglio Nazionale delle Ricerche. Monografie Mathematiche 4), VI + 322 p., Roma, Edizioni Cremonese, 1957.

Le but de l'auteur est de présenter un traité de la théorie des matrices en langue italienne, qui suscite l'intérêt des cultivateurs des mathématiques pures et est en même

temps utile à ceux qui appliquent le calcul des matrices à des fins "opératives et techniques". Il accomplit ce but par une originalité remarquable tant dans le choix des sujets particuliers traités que dans la présentation.

Le livre est divisé en quatre chapitres. Le premier, intitulé "Propriétés formelles", contient les définitions fondamentales et des problèmes à la solution desquels on n'a besoin que des opérations rationnelles. Paragraphes: 1. Définitions et notations. 2. Somme et produit. 3. Réduction à forme triangulaire. 4. Les équations $AX = B$, $YA = C$. 5. Symétrie et antisymétrie. Diagonalisation. 6. Normalisation. Valeur maximum d'une déterminante. 7. Formes quadratiques et hermitiennes. Matrices définies ou semidéfinies. 8. Permutabilité et orthodiagonalisation. 9. Notion sur les anneaux et corps numériques. 10. Matrices aux éléments polynômes. 11. Matrices entières. 12. Notions sur les Algèbres abstraites. 13. Dérivation et intégration. 14. Produit intégral. 15. Espace numérique, espace vectoriel, espace projectif. — L'auteur définit les matrices et leurs sommes et produits d'une façon dogmatique, sans aucune motivation par les substitutions ou transformations linéaires; en effet, les espaces vectoriels ne sont qu'effleurés dans le dernier paragraphe. Il ne s'agit pas de telles notions que la matrice d'une transformation linéaire par rapport à de différentes bases, ce qui est d'autant plus étonnant que dans le § 12 on traite de questions particulières telles que les tableaux de multiplication des Algèbres abstraites. Dans une période du développement des Mathématiques où les espaces linéaires et leurs opérateurs sont en premier rang des recherches, cette attitude de l'auteur paraît presque archaïque.

Chapitre II, sur les "Propriétés de structure", traite des formes canoniques de JORDAN et plusieurs applications intéressantes. Paragraphes: 1. Equations et racines caractéristiques. 2. Théorèmes de LAPPO—DANILEVSKY et de FROBENIUS. (Il s'agit ici des racines caractéristiques des matrices aux éléments positifs et des matrices qui sont majorées par de telles matrices.) 3. Coordonnées orthogonales dans l'espace S_n. Maxima et minima des formes quadratiques. 4. Transformations par contragrédience ou par similitude. (C'est ici qu'on démontre, entre autres, la forme canonique de JORDAN.) 5. Permutabilité avec une matrice donnée. 6. Inverse, résolvante, formule de SYLVESTER et de FROBENIUS. Algèbres commutatives.

Le Chapitre III, sur les "Approximations et limitations des racines caractéristiques", est constitué des paragraphes suivants: 1. Approximation de la racine dominante. 2. Théorèmes de MÜLLER, OSTROWSKI, LÉVY—HADAMARD et conséquences. 3. Représentation du spectre dans le plan complexe. 4. Matrices à racine caractéristique de module inférieur à l'unité. Enfin, le Chapitre IV, intitulé "Fonctions de matrices", embrasse le paragraphes: 1. Séries de matrices. 2. Fonctions dans une algèbre complexe douée de module (c'est-à-dire contenant un élément unité). 3. Fonctions analytiques et fonctions holomorphes dans une algèbre de matrices douée de module. — L'auteur esquisse ici quelques résultats de SPAMPINATO et de lui-même. Il est à regretter qu'il ne mentionne pas ici les résultats voisins ou même plus généraux de quelques autres auteurs, comme par exemple l'article de E. R. LORCH sur les fonctions analytiques dans des algèbres abéliennes normées (de dimension quelconque), *Transactions Amer. Math. Soc.*, 54 (1943), 414—425.

Un index bibliographique de 8 pages et un index analytique détaillé terminent le livre.

Béla Sz.-Nagy (Szeged)

„KULTURA" BUDAPEST, OFFERS

ACTA MATHEMATICA ACADEMIAE SCIENTIARUM HUNGARICAE, Budapest

Mostly reprinted. Vols. 1—18. 1950—1967,
with HUNGARICA ACTA MATHEMATICA, Vol. 1, 1949,
and Supplement to vol. 5.

clothbound US $ 323.—; paperbound, resp. in original issues US $ 285.—

ACTA SCIENTIARUM MATHEMATICARUM, Szeged

Mostly reprinted. Vols. 1—28, 1922—1967.

clothbound US $ 464.—; paperbound, resp. in original issues US $ 406.—

PUBLICATIONES MATHEMATICAE, Debrecen

Partly reprinted. Vols. 1—14, 1949—1967

clothbound US $ 210.—; paperbound, resp. in original issues US $ 182.—

ANNALES UNIVERSITATIS SCIENTIARUM BUDAPESTIENSIS DE R. EÖTVÖS NOMINATAE,

Sectio Mathematica
Mostly reprinted. Vols. 1—9, 1958—1966, including memorial vol. ¾, devoted to L. Fejér

clothbound US $ 90.—; paperbound US $ 72.—

PUBLICATIONS OF THE MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES
(A Magyar Tudományos Akadémia Matematikai Kutató Intézetének Közleményei)

Partly reprinted, published mostly in congress languages
Old Series: Vols. 1—3, 1952—1954 (all published)
New Series: Vols. 1—9, 1956—1964 (all published)

clothbound US $ 134.—; paperbound, resp. in original issues US $ 110.—

STUDIA SCIENTIARUM MATHEMATICARUM HUNGARICA, Budapest

Vols. 1—2, 1966—1967

clothbound US $ 28.—; in original issues US $ 24.—

MATEMATIKAI ÉS FIZIKAI LAPOK, Budapest

Mostly reprinted (available in October, 1968). Vols. 1—50, 1892—1943, all published, with General Index

clothbound US $ 850.—, paperbound, resp. in original issues US $ 750.—

Prepublication price, valid until June 30, 1968:
clothbound US $ 800.—, paperbound, resp. in original issues US $ 700.—

Published by the L. Eötvös Mathematical and Physical Association in Hungarian, since 1920 contains also ample summaries in German language.
Mathematical editors: G. Rados (1892—1913), L. Fejér (1914—1932), D. König (1933—1943).

MATEMATIKAI LAPOK, Budapest

Partly reprinted. Vols. 1—18, 1949/50—1967

clothbound US $ 196.—, paperbound, resp. in original issues US $ 160.—

Mathematical quarterly, published by the Bolyai Mathematical Society in Hungarian, with summaries in congress languages.

SOVIET MATHEMATICAL REPRINTS

TRUDY SEMINARA PO VEKTORNOMU I TENZORNOMU ANALIZU

Abhandlungen aus dem Seminar für Vektor- und Tensoranalysis. Mémoires du Séminaire pour l'Analyse vectorielle et tensorielle. Moscow-Leningrad, 1933—1966

clothbound US $ 240.—

Vols. 1—4 are published chiefly in Western languages. Vol. 4. contains the proceedings of the 1st International Conference for Tensor Differential Geometry, held in Moscow, 1934.
Editors: Professor V. F. Kagan and P. K. Razhevskij

Single volumes of all above periodicals are available. Subscriptions to forthcoming volumes may be also entered.

„KULTURA"

**Hungarian Trading Company for Books and Newpapers,
Back issues Department,**

BUDAPEST 62, P. O. B. 149, Hungary

Orders and inquiries should be sent to above address, directly, or through any international scientific bookseller.